Vulnerability Summary for the Week of July 12, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 07/19/2021 12:14 PM EDT

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of July 12, 2021

07/19/2021 06:50 AM EDT

Original release date: July 19, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
echobh -- sharecare	Echo ShareCare 8.15.5 is susceptible to SQL injection vulnerabilities when processing remote input from both authenticated and unauthenticated users, leading to the ability to bypass authentication, exfiltrate Structured Query Language (SQL) records, and manipulate data.	2021-07-13	7.5	CVE-2021-33578 MISC
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. It does not perform authentication or authorization checks when accessing a subset of sensitive resources, leading to the ability for unauthenticated users to access pages that are vulnerable to attacks such as SQL injection.	2021-07-13	7.5	CVE-2021-36124 MISC
espruino -- espruino	Buffer overflow vulnerability in function jsvGetStringChars in Espruino before RELEASE_2V09, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22884 MISC
fortinet -- forticlient	An improper symlink following in FortiClient for Mac 6.4.3 and below may allow an non-privileged user to execute arbitrary privileged shell commands during installation phase.	2021-07-12	7.2	CVE-2021-26089 CONFIRM
fortinet -- fortimail	A missing cryptographic step in the implementation of the hash digest algorithm in FortiMail 6.4.0 through 6.4.4, and 6.2.0 through 6.2.7 may allow an unauthenticated attacker to tamper with signed URLs by appending further data which allows bypass of signature verification.	2021-07-09	7.5	CVE-2021-24020 CONFIRM
fortinet -- fortimail	Multiple improper neutralization of special elements of SQL commands vulnerabilities in FortiMail before 6.4.4 may allow a non-authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	7.5	CVE-2021-24007 CONFIRM
golang -- go	golang/go in 1.0.2 fixes all.bash on shared machines. dotest() in src/pkg/debug/gosym/pclntab_test.go creates a temporary file with predicable name and executes it as shell script.	2021-07-09	7.5	CVE-2012-2666 MISC MISC MISC MISC
google -- android	In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181346550	2021-07-14	7.8	CVE-2021-0596 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In setNiNotification of GpsNetInitiatedHandler.java, there is a possible permissions bypass due to an empty mutable PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-154319182	2021-07-14	7.2	CVE-2020-0417 MISC
google -- android	In flv extractor, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187161771	2021-07-14	7.2	CVE-2021-0577 MISC
google -- android	In Factory::CreateStrictFunctionMap of factory.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-167389063	2021-07-14	10	CVE-2021-0515 MISC
google -- android	In beginWrite and beginRead of MessageQueueBase.h, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-184963385	2021-07-14	7.2	CVE-2021-0585 MISC
google -- android	In onCreate of ConfirmConnectActivity, there is a possible remote bypass of user consent due to improper input validation. This could lead to remote (proximal, NFC) escalation of privilege allowing an attacker to deceive a user into allowing a Bluetooth connection with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176445224	2021-07-14	7.9	CVE-2021-0594 MISC
google -- android	In StreamOut::prepareForWriting of StreamOut.cpp, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-185259758	2021-07-14	7.2	CVE-2021-0587 MISC
google -- android	In BTM_TryAllocateSCN of btm_scn.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-180939982	2021-07-14	7.2	CVE-2021-0589 MISC
google -- android	In various functions in WideVine, there are possible out of bounds writes due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-188061006	2021-07-14	9.3	CVE-2021-0592 MISC
google -- android	In several functions of the V8 library, there is a possible use after free due to a race condition. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-9 Android-11 Android-8.1Android ID: A-162604069	2021-07-14	9.3	CVE-2021-0514 MISC
google -- android	In onCreateOptionsMenu of WifiNetworkDetailsFragment.java, there is a possible way for guest users to view and modify Wi-Fi settings for all configured APs due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-177573895	2021-07-14	7.2	CVE-2021-0602 MISC
halo -- halo	Remote Code Executon vulnerability in Halo 0.4.3 via the remoteAddr and themeName parameters.	2021-07-12	7.5	CVE-2020-18980 MISC
jsish -- jsish	Integer overflow vulnerability in function Jsi_ObjSetLength in jsish before 3.0.6, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22875 MISC MISC
jsish -- jsish	Integer overflow vulnerability in function Jsi_ObjArraySizer in jsish before 3.0.8, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22874 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jsish -- jsish	Buffer overflow vulnerability in function NumberToPrecisionCmd in jsish before 3.0.7, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22873 MISC
kaseya -- vsa	Kaseya VSA before 9.5.5 allows remote code execution.	2021-07-09	7.5	CVE-2021-30118 MISC
kramerav -- viaware	KramerAV VIAWare, all tested versions, allow privilege escalation through misconfiguration of sudo. Sudoers permits running of multiple dangerous commands, including unzip, systemctl and dpkg.	2021-07-12	7.5	CVE-2021-35064 MISC
linux -- linux_kernel	An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-07-09	7.2	CVE-2021-3612 MISC MISC
linuxptp_project -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1.	2021-07-09	8	CVE-2021-3570 MISC DEBIAN FEDORA FEDORA
metinfo -- metinfo	SQL Injection vulnerability in Metinfo 7.0.0beta in index.php.	2021-07-12	7.5	CVE-2020-21132 MISC MISC
metinfo -- metinfo	SQL Injection vulnerability in Metinfo 7.0.0 beta in member/getpassword.php?lang=cn&a=dovalid.	2021-07-12	7.5	CVE-2020-21133 MISC MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-34473.	2021-07-14	7.5	CVE-2021-31206 MISC
microsoft -- windows_10	Windows Kernel Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31979, CVE-2021-34514.	2021-07-14	7.2	CVE-2021-33771 MISC
microsoft -- windows_10	Windows Security Account Manager Remote Protocol Security Feature Bypass Vulnerability	2021-07-14	7.5	CVE-2021-33757 MISC
microsoft -- windows_10	Windows Secure Kernel Mode Security Feature Bypass Vulnerability	2021-07-14	7.2	CVE-2021-33744 MISC
microsoft -- windows_10	Windows Kernel Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33771, CVE-2021-34514.	2021-07-14	7.2	CVE-2021-31979 MISC
microsoft -- windows_10	Windows Media Remote Code Execution Vulnerability	2021-07-14	9.3	CVE-2021-33740 MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server supports application specific tokens for authentication purposes. These tokens are supposed to be granted to a specific applications (e.g. DAV sync clients), and can also be configured by the user to not have any filesystem access. Due to a lacking permission check, the tokens were able to change their own permissions in versions prior to 19.0.13, 20.0.11, and 21.0.3. Thus fileystem limited tokens were able to grant themselves access to the filesystem. The issue is patched in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds aside from upgrading.	2021-07-12	7.5	CVE-2021-32688 MISC CONFIRM MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, webauthn tokens were not deleted after a user has been deleted. If a victim reused an earlier used username, the previous user could gain access to their account. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	7.5	CVE-2021-32726 MISC MISC CONFIRM
ninjateam -- filebird	The Filebird Plugin 4.7.3 introduced a SQL injection vulnerability as it is making SQL queries without escaping user input data from a HTTP post request. This is a major vulnerability as the user input is not escaped and passed directly to the get_col function and it allows SQL injection. The Rest API endpoint which invokes this function also does not have any required permissions/authentication and can be accessed by an anonymous user.	2021-07-12	7.5	CVE-2021-24385 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
putil-merge_project -- putil-merge	Prototype pollution vulnerability in 'putil-merge' versions1.0.0 through 3.6.6 allows attacker to cause a denial of service and may lead to remote code execution.	2021-07-14	7.5	CVE-2021-25953 MISC
python -- pillow	Pillow through 8.2.0 and PIL (aka Python Imaging Library) through 1.1.7 allow an attacker to pass controlled parameters directly into a convert function to trigger a buffer overflow in Convert.c.	2021-07-13	7.5	CVE-2021-34552 MISC MISC
qualcomm -- apq8009w_firmware	Buffer overflow in modem due to improper array index check before copying into it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	2021-07-13	10	CVE-2020-11307 CONFIRM
qualcomm -- apq8017_firmware	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1890 CONFIRM
qualcomm -- apq8017_firmware	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1886 CONFIRM
qualcomm -- apq8017_firmware	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1889 CONFIRM
qualcomm -- apq8017_firmware	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1888 CONFIRM
qualcomm -- aqt1000_firmware	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-07-13	7.2	CVE-2021-1931 CONFIRM
qualcomm -- aqt1000_firmware	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1940 CONFIRM
qualcomm -- aqt1000_firmware	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	10	CVE-2021-1965 CONFIRM
sap -- netweaver_as_abap	A function module of SAP NetWeaver AS ABAP (Reconciliation Framework), versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 75A, 75B, 75B, 75C, 75D, 75E, 75F, allows a high privileged attacker to inject code that can be executed by the application. An attacker could thereby delete some critical information and could make the SAP system completely unavailable.	2021-07-14	7.5	CVE-2021-33678 MISC MISC
solarwinds -- dameware_mini_remote_control	In SolarWinds DameWare Mini Remote Control Server 12.0.1.200, insecure file permissions allow file deletion as SYSTEM.	2021-07-13	9.4	CVE-2021-31217 MISC MISC
totaljs -- total.js	The package total.js before 3.4.9 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.	2021-07-12	7.5	CVE-2021-23389 MISC MISC MISC
totaljs -- total4	The package total4 before 0.0.43 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.	2021-07-12	7.5	CVE-2021-23390 MISC MISC MISC
wms_project -- wms	SQL Injection in WMS v1.0 allows remote attackers to execute arbitrary code via the "username" parameter in the component "chkuser.php".	2021-07-12	7.5	CVE-2020-18544 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpdevart -- poll\,_survey\,_questionnaire_and_voting_system	The Poll, Survey, Questionnaire and Voting system WordPress plugin before 1.5.3 did not sanitise, escape or validate the date_answers[] POST parameter before using it in a SQL statement when sending a Poll result, allowing unauthenticated users to perform SQL Injection attacks	2021-07-12	7.5	CVE-2021-24442 CONFIRM MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- ant	When reading a specially crafted TAR archive an Apache Ant build can be made to allocate large amounts of memory that finally leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	2021-07-14	4.3	CVE-2021-36373 MISC MISC MLIST MLIST MLIST
apache -- ant	When reading a specially crafted ZIP archive, or a derived formats, an Apache Ant build can be made to allocate large amounts of memory that leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Commonly used derived formats from ZIP archives are for instance JAR files and many office files. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	2021-07-14	4.3	CVE-2021-36374 MISC MISC MLIST MLIST MLIST
apache -- tomcat	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.	2021-07-12	5	CVE-2021-33037 MISC
apache -- tomcat	A vulnerability in Apache Tomcat allows an attacker to remotely trigger a denial of service. An error introduced as part of a change to improve error handling during non-blocking I/O meant that the error flag associated with the Request object was not reset between requests. This meant that once a non-blocking I/O error occurred, all future requests handled by that request object would fail. Users were able to trigger non-blocking I/O errors, e.g. by dropping a connection, thereby creating the possibility of triggering a DoS. Applications that do not use non-blocking I/O are not exposed to this vulnerability. This issue affects Apache Tomcat 10.0.3 to 10.0.4; 9.0.44; 8.5.64.	2021-07-12	5	CVE-2021-30639 MISC MLIST MLIST
artifex -- mujs	Buffer overflow vulnerability in function jsG_markobject in jsgc.c in mujs before 1.0.8, allows remote attackers to cause a denial of service.	2021-07-13	5	CVE-2020-22886 MISC
artifex -- mujs	Buffer overflow vulnerability in mujs before 1.0.8 due to recursion in the GC scanning phase, allows remote attackers to cause a denial of service.	2021-07-13	5	CVE-2020-22885 MISC
autodesk -- design_review	A maliciously crafted PDF, PICT or TIFF file can be used to write beyond the allocated buffer while parsing PDF, PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27036 MISC
autodesk -- design_review	A maliciously crafted TIFF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read and write beyond allocated boundaries when parsing the TIFF file. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27039 MISC
autodesk -- design_review	A Type Confusion vulnerability in Autodesk 2018, 2017, 2013, 2012, 2011 can occur when processing a maliciously crafted PDF file. An attacker can leverage this to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27038 MISC
autodesk -- design_review	A maliciously crafted PNG, PDF or DWF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be used to attempt to free an object that has already been freed while parsing them. This vulnerability can be exploited by remote attackers to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27037 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- design_review	A heap-based buffer overflow could occur while parsing PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27034 MISC
autodesk -- design_review	A maliciously crafted TIFF, PDF, PICT or DWF files in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read beyond allocated boundaries when parsing the TIFF, PDF, PICT or DWF files. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27035 MISC
axiosys -- bento4	A buffer overflow vulnerability in Ap4ElstAtom.cpp of Bento 1.5.1-628 leads to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19719 MISC
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a direct copy to NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19722 MISC
axiosys -- bento4	An unhandled memory allocation failure in Core/AP4IkmsAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19720 MISC
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19718 MISC
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap48bdlAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19717 MISC
axiosys -- bento4	A heap buffer overflow vulnerability in Ap4TrunAtom.cpp of Bento 1.5.1-628 may lead to an out-of-bounds write while running mp42aac, leading to system crashes and a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19721 MISC
baidu -- umeditor	Cross Site Scripting (XSS) vulnerability in umeditor v1.2.3 via /public/common/umeditor/php/getcontent.php.	2021-07-14	4.3	CVE-2020-18145 MISC
bookingcore -- booking_core	The “Subscribe” feature in Ultimate Booking System Booking Core 1.7.0 is vulnerable to CSV formula injection. The input containing the excel formula is not being sanitized by the application. As a result when admin in backend download and open the csv, content of the cells are executed.	2021-07-14	6.8	CVE-2020-25445 MISC
bookingcore -- booking_core	Cross Site Request Forgery (CSRF) vulnerability in Booking Core - Ultimate Booking System Booking Core 1.7.0 . The CSRF token is not being validated when the request is sent as a GET method. This results in an unauthorized change in the user's email ID, which can later be used to reset the password. The new password will be sent to a modified email ID.	2021-07-14	4.3	CVE-2020-27379 MISC
brave -- brave	In Brave Desktop between versions 1.17 and 1.26.60, when adblocking is enabled and a proxy browser extension is installed, the CNAME adblocking feature issues DNS requests that used the system DNS settings instead of the extension's proxy settings, resulting in possible information disclosure.	2021-07-12	4.3	CVE-2021-22916 MISC
brave -- browser	Brave Browser Desktop between versions 1.17 and 1.20 is vulnerable to information disclosure by way of DNS requests in Tor windows not flowing through Tor if adblocking was enabled.	2021-07-12	4.3	CVE-2021-22917 MISC
codeblab -- glass	The Glass WordPress plugin through 1.3.2 does not sanitise or escape its "Glass Pages" setting before outputting in a page, leading to a Stored Cross-Site Scripting issue. Furthermore, the plugin did not have CSRF check in place when saving its settings, allowing the issue to be exploited via a CSRF attack.	2021-07-12	4.3	CVE-2021-24434 CONFIRM
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	2021-07-12	4.6	CVE-2021-21590 MISC
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 do not exit on failed Initialization. A local authenticated Service user could potentially exploit this vulnerability to escalate privileges.	2021-07-12	4.6	CVE-2021-21589 MISC
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	2021-07-12	4.6	CVE-2021-21591 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- powerflex_presentation_server	Dell EMC PowerFlex, v3.5.x contain a Cross-Site WebSocket Hijacking Vulnerability in the Presentation Server/WebUI. An unauthenticated attacker could potentially exploit this vulnerability by tricking the user into performing unwanted actions on the Presentation Server and perform which may lead to configuration changes.	2021-07-12	4.3	CVE-2021-21588 MISC
delta_project -- delta	dandavison delta before 0.8.3 on Windows resolves an executable's pathname as a relative path from the current directory.	2021-07-13	4.4	CVE-2021-36376 CONFIRM MISC MISC
devolutions -- devolutions_server	Devolutions Server before 2021.1.18, and LTS before 2020.3.20, allows attackers to intercept private keys via a man-in-the-middle attack against the connections/partial endpoint (which accepts cleartext).	2021-07-12	4.3	CVE-2021-36382 MISC
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The TextReader feature in General/TextReader/TextReader.cfm is susceptible to a local file inclusion vulnerability when processing remote input in the textFile parameter from an authenticated user, leading to the ability to read arbitrary files on the server filesystems as well any files accessible via Universal Naming Convention (UNC) paths.	2021-07-13	4	CVE-2021-36123 MISC
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The UnzipFile feature in Access/EligFeedParse_Sup/UnzipFile_Upd.cfm is susceptible to a command argument injection vulnerability when processing remote input in the zippass parameter from an authenticated user, leading to the ability to inject arbitrary arguments to 7z.exe.	2021-07-13	6.5	CVE-2021-36122 MISC
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The file-upload feature in Access/DownloadFeed_Mnt/FileUpload_Upd.cfm is susceptible to an unrestricted upload vulnerability via the name1 parameter, when processing remote input from an authenticated user, leading to the ability for arbitrary files to be written to arbitrary filesystem locations via ../ Directory Traversal on the Z: drive (a hard-coded drive letter where ShareCare application files reside) and remote code execution as the ShareCare service user (NT AUTHORITY\SYSTEM).	2021-07-13	6.5	CVE-2021-36121 MISC
edgexfoundry -- edgex_foundry	EdgeX Foundry is an open source project for building a common open framework for internet-of-things edge computing. A vulnerability exists in the Edinburgh, Fuji, Geneva, and Hanoi versions of the software. When the EdgeX API gateway is configured for OAuth2 authentication and a proxy user is created, the client_id and client_secret required to obtain an OAuth2 authentication token are set to the username of the proxy user. A remote network attacker can then perform a dictionary-based password attack on the OAuth2 token endpoint of the API gateway to obtain an OAuth2 authentication token and use that token to make authenticated calls to EdgeX microservices from an untrusted network. OAuth2 is the default authentication method in EdgeX Edinburgh release. The default authentication method was changed to JWT in Fuji and later releases. Users should upgrade to the EdgeX Ireland release to obtain the fix. The OAuth2 authentication method is disabled in Ireland release. If unable to upgrade and OAuth2 authentication is required, users should create OAuth2 users directly using the Kong admin API and forgo the use of the `security-proxy-setup` tool to create OAuth2 users.	2021-07-09	5.8	CVE-2021-32753 MISC CONFIRM
edifecs -- transaction_management	In Edifecs Transaction Management through 2021-07-12, an unauthenticated user can inject arbitrary text into a user's browser via logon.jsp?logon_error= on the login screen of the Web application.	2021-07-12	5	CVE-2021-36381 MISC MISC
element-it -- http_commander	A Directory Traversal vulnerability in the Unzip feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to write files to arbitrary directories via relative paths in ZIP archives.	2021-07-14	4	CVE-2021-33211 MISC MISC
element-it -- http_commander	An SSRF vulnerability in the "Upload from URL" feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to retrieve HTTP and FTP files from the internal server network by inserting an internal address.	2021-07-14	4	CVE-2021-33213 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
esri -- arcgis_server	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	2021-07-10	4.3	CVE-2021-29107 CONFIRM
esri -- arcgis_server	A reflected Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	2021-07-10	4.3	CVE-2021-29106 CONFIRM
esri -- arcgis_server	A Server-Side Request Forgery (SSRF) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote, unauthenticated attacker to forge GET requests to arbitrary URLs from the system, potentially leading to network enumeration or facilitating other attacks.	2021-07-11	6.4	CVE-2021-29102 CONFIRM
esri -- arcgis_server	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	2021-07-11	4.3	CVE-2021-29104 CONFIRM
esri -- arcgis_server	A reflected Cross Site Scripting (XXS) vulnerability in ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	2021-07-11	4.3	CVE-2021-29103 CONFIRM
eventespresso -- event_espresso	A cross-site scripting (XSS) vulnerability in wp-content/plugins/event-espresso-core-reg/admin_pages/messages/templates/ee_msg_admin_overview.template.php in the Event Espresso Core plugin before 4.10.7.p for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2021-07-13	4.3	CVE-2020-26153 MISC MISC
exiv2 -- exiv2	A buffer overflow vulnerability in the Databuf function in types.cpp of Exiv2 v0.27.1 leads to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19716 MISC
exiv2 -- exiv2	An integer overflow vulnerability in the getUShort function of Exiv2 0.27.1 results in segmentation faults within the application, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19715 MISC
fetchdesigns -- sign-up_sheets	The Sign-up Sheets WordPress plugin before 1.0.14 does not not sanitise or validate the Sheet title when generating the CSV to export, which could lead to a CSV injection issue	2021-07-12	6	CVE-2021-24441 CONFIRM
fortinet -- fortiap	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments.	2021-07-09	4.6	CVE-2021-26106 CONFIRM
fortinet -- fortimail	A missing release of memory after its effective lifetime vulnerability in the Webmail of FortiMail 6.4.0 through 6.4.4 and 6.2.0 through 6.2.6 may allow an unauthenticated remote attacker to exhaust available memory via specifically crafted login requests.	2021-07-12	5	CVE-2021-26090 CONFIRM
fortinet -- fortimail	An improper neutralization of special elements used in an OS Command vulnerability in the administrative interface of FortiMail before 6.4.4 may allow an authenticated attacker to execute unauthorized commands via specifically crafted HTTP requests.	2021-07-12	6.5	CVE-2021-24015 CONFIRM
fortinet -- fortimail	A missing cryptographic step in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an unauthenticated attacker who intercepts the encrypted messages to manipulate them in such a way that makes the tampering and the recovery of the plaintexts possible.	2021-07-09	5	CVE-2021-26100 CONFIRM
fortinet -- fortimail	Multiple Path traversal vulnerabilities in the Webmail of FortiMail before 6.4.4 may allow a regular user to obtain unauthorized access to files and data via specifically crafted web requests.	2021-07-12	4	CVE-2021-24013 CONFIRM
fortinet -- fortimail	Missing cryptographic steps in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an attacker who comes in possession of the encrypted master keys to compromise their confidentiality by observing a few invariant properties of the ciphertext.	2021-07-12	4	CVE-2021-26099 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortimail	Multiple instances of incorrect calculation of buffer size in the Webmail and Administrative interface of FortiMail before 6.4.5 may allow an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	6.5	CVE-2021-22129 CONFIRM
fortinet -- fortisandbox	A concurrent execution using shared resource with improper synchronization ('race condition') in the command shell of FortiSandbox before 3.2.2 may allow an authenticated attacker to bring the system into an unresponsive state via specifically orchestrated sequences of commands.	2021-07-09	6.3	CVE-2020-29014 CONFIRM
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 produce incorrect PDF document signatures because the certificate name, document owner, and signature author are mishandled.	2021-07-09	4.3	CVE-2021-33795 MISC
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write via a crafted /Size key in the Trailer dictionary.	2021-07-09	6.8	CVE-2021-33792 MISC
getambassador -- emissary-ingress	Emissary-Ingress (formerly Ambassador API Gateway) through 1.13.9 allows attackers to bypass client certificate requirements (i.e., mTLS cert_required) on backend upstreams when more than one TLSContext is defined and at least one configuration exists that does not require client certificate authentication. The attacker must send an SNI specifying an unprotected backend and an HTTP Host header specifying a protected backend. (2.x versions are unaffected. 1.x versions are unaffected with certain configuration settings involving prune_unreachable_routes and a wildcard Host resource.)	2021-07-09	4.3	CVE-2021-36371 MISC MISC
google -- android	In handleSendStatusChangeBroadcast of WifiDisplayAdapter.java, there is a possible leak of location-sensitive data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176541017	2021-07-14	4.9	CVE-2021-0518 MISC
google -- android	In onCreate of DevicePickerFragment.java, there is a possible way to trick the user to select an unwanted bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-182584940	2021-07-14	6.9	CVE-2021-0586 MISC
google -- android	In processInboundMessage of MceStateMachine.java, there is a possible SMS disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-177238342	2021-07-14	4.9	CVE-2021-0588 MISC
google -- android	In onCreate of PermissionActivity.java, there is a possible permission bypass due to Confusing UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174495520	2021-07-14	4.4	CVE-2021-0441 MISC
google -- android	In onCreate of DeviceAdminAdd.java, there is a possible way to mislead a user to activate a device admin app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-179042963	2021-07-14	6.9	CVE-2021-0600 MISC
google -- android	In encodeFrames of avc_enc_fuzzer.cpp, there is a possible out of bounds write due to a double free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-180643802	2021-07-14	4.9	CVE-2021-0601 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onCreate of ContactSelectionActivity.java, there is a possible way to get access to contacts without permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-182809425	2021-07-14	4.4	CVE-2021-0603 MISC
google -- android	In sendNetworkConditionsBroadcast of NetworkMonitor.java, there is a possible way for a privileged app to receive WiFi BSSID and SSID without location permissions due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-175213041	2021-07-14	4.9	CVE-2021-0590 MISC
google -- android	In onPackageAddedInternal of PermissionManagerService.java, there is possible access to external storage due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-171430330	2021-07-14	4.6	CVE-2021-0486 MISC
google -- android	In scheduleTimeoutLocked of NotificationRecord.java, there is a possible disclosure of a sensitive identifier via broadcasted intent due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175614289	2021-07-14	4.9	CVE-2021-0599 MISC
google -- android	In notifyProfileAdded and notifyProfileRemoved of SipService.java, there is a possible way to retrieve SIP account names due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-176496502	2021-07-14	4.9	CVE-2021-0597 MISC
halo -- halo	File Deletion vulnerability in Halo 0.4.3 via delBackup.	2021-07-12	6.4	CVE-2020-19038 MISC
halo -- halo	Incorrect Access Control vulnearbility in Halo 0.4.3, which allows a malicious user to bypass encrption to view encrpted articles via cookies.	2021-07-12	5	CVE-2020-19037 MISC
halo -- halo	Cross Siste Scripting (XSS) vulnerablity in Halo 0.4.3 via the X-forwarded-for Header parameter.	2021-07-12	4.3	CVE-2020-18979 MISC
halo -- halo	SSRF vulnerability in Halo <=1.3.2 exists in the SMTP configuration, which can detect the server intranet.	2021-07-12	5	CVE-2020-23079 MISC
hms-networks -- ecatcher	In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation.	2021-07-09	6	CVE-2021-33214 MISC MISC MISC MISC
hmtalk -- daviewindy	DaviewIndy v8.98.7.0 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed format file that is mishandled by DaviewIndy. Attackers could exploit this and arbitrary code execution.	2021-07-12	6.8	CVE-2020-7872 MISC
huawei -- harmonyos	A component of the HarmonyOS 2.0 has a Null Pointer Dereference Vulnerability. Local attackers may exploit this vulnerability to cause system denial of service.	2021-07-14	4.9	CVE-2021-22318 MISC
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could allow an authenticated user gain escalated privilesges due to improper application permissions. IBM X-Force ID: 196308.	2021-07-13	6.5	CVE-2021-20423 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could disclose sensitive information to a malicious attacker by accessing data stored in memory. IBM X-Force ID: 196304.	2021-07-13	5	CVE-2021-20422 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195361.	2021-07-13	4.3	CVE-2021-20369 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195031.	2021-07-13	5	CVE-2021-20360 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. X-Force ID: 196309.	2021-07-13	4	CVE-2021-20424 XF CONFIRM
ibm -- event_streams	IBM Event Streams 10.0, 10.1, 10.2, and 10.3 could allow a user the CA private key to create their own certificates and deploy them in the cluster and gain privileges of another user. IBM X-Force ID: 203450.	2021-07-12	6.5	CVE-2021-29792 CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 3.0.0.2 could allow a user to bruce force sensitive information due to not properly limiting the number of interactions. IBM X-Force ID: 196216.	2021-07-12	4	CVE-2021-20414 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 200966.	2021-07-09	4.3	CVE-2021-29712 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 201164.	2021-07-09	6.5	CVE-2021-29730 XF CONFIRM
ibm -- mq_appliance	IBM MQ Appliance 9.1 and 9.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 191815.	2021-07-12	6.8	CVE-2020-4938 CONFIRM XF
ibm -- tivoli_netcool\/impact	IBM Tivoli Netcool/Impact 7.1.0.20 and 7.1.0.21 uses an insecure SSH server configuration which enables weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 203556.	2021-07-12	5	CVE-2021-29794 XF CONFIRM
icinga -- icinga	Icinga Web 2 is an open source monitoring web interface, framework, and command-line interface. A vulnerability in which custom variables are exposed to unauthorized users exists between versions 2.0.0 and 2.8.2. Custom variables are user-defined keys and values on configuration objects in Icinga 2. These are commonly used to reference secrets in other configurations such as check commands to be able to authenticate with a service being checked. Icinga Web 2 displays these custom variables to logged in users with access to said hosts or services. In order to protect the secrets from being visible to anyone, it's possible to setup protection rules and blacklists in a user's role. Protection rules result in `***` being shown instead of the original value, the key will remain. Backlists will hide a custom variable entirely from the user. Besides using the UI, custom variables can also be accessed differently by using an undocumented URL parameter. By adding a parameter to the affected routes, Icinga Web 2 will show these columns additionally in the respective list. This parameter is also respected when exporting to JSON or CSV. Protection rules and blacklists however have no effect in this case. Custom variables are shown as-is in the result. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, one may set up a restriction to hide hosts and services with the custom variable in question.	2021-07-12	4	CVE-2021-32747 MISC MISC CONFIRM MISC
ipfire -- ipfire	Lightning Wire Labs IPFire 2.21 (x86_64) - Core Update 130 is affected by: Cross Site Scripting (XSS). The impact is: Session Hijacking (local). The component is: Affected at Routing configuration via the "Remark" text box or "remark" parameter. The attack vector is: Attacker need to craft the malicious javascript code.	2021-07-12	4.3	CVE-2020-19204 MISC MISC
jsish -- jsish	Stack overflow vulnerability in function jsi_evalcode_sub in jsish before 3.0.18, allows remote attackers to cause a Denial of Service via a crafted value to the execute parameter.	2021-07-13	5	CVE-2020-22907 MISC
kaseya -- vsa	SQL injection exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30117 MISC
kaseya -- vsa	Local file inclusion exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30121 MISC
kaseya -- vsa	Kaseya VSA through 9.5.7 allows attackers to bypass the 2FA requirement.	2021-07-09	5	CVE-2021-30120 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kaseya -- vsa	An XML External Entity (XXE) issue exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30201 MISC
linecorp -- line	LINE client for iOS before 10.16.3 allows cross site script with specific header in WebView.	2021-07-13	4.3	CVE-2021-36214 MISC
linuxfoundation -- grpc_swift	Mismanaged state in GRPCWebToHTTP2ServerCodec.swift in gRPC Swift 1.1.0 and 1.1.1 allows remote attackers to deny service by sending malformed requests.	2021-07-09	5	CVE-2021-36153 MISC MISC MISC
linuxfoundation -- grpc_swift	LengthPrefixedMessageReader in gRPC Swift 1.1.0 and earlier allocates buffers of arbitrary length, which allows remote attackers to cause uncontrolled resource consumption and deny service.	2021-07-09	5	CVE-2021-36155 MISC MISC MISC
linuxfoundation -- grpc_swift	HTTP2ToRawGRPCServerCodec in gRPC Swift 1.1.1 and earlier allows remote attackers to deny service via the delivery of many small messages within a single HTTP/2 frame, leading to Uncontrolled Recursion and stack consumption.	2021-07-09	5	CVE-2021-36154 MISC MISC MISC
linuxptp_project -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. When ptp4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1.	2021-07-09	5.5	CVE-2021-3571 MISC FEDORA FEDORA
metinfo -- metinfo	SQL Injection vulnerability in MetInfo 7.0.0beta via admin/?n=language&c=language_web&a=doAddLanguage.	2021-07-12	6.5	CVE-2020-21131 MISC MISC
microfocus -- netiq_advanced_authentication	Multi-Factor Authentication (MFA) functionality can be bypassed, allowing the use of single factor authentication in NetIQ Advanced Authentication versions prior to 6.3 SP4 Patch 1.	2021-07-12	4	CVE-2021-22515 CONFIRM
microsoft -- bing	Microsoft Bing Search Spoofing Vulnerability	2021-07-14	4.3	CVE-2021-33753 MISC
microsoft -- exchange_server	Microsoft Exchange Information Disclosure Vulnerability	2021-07-14	5	CVE-2021-33766 MISC MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31206, CVE-2021-34473.	2021-07-14	6.5	CVE-2021-31196 MISC
microsoft -- exchange_server	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34470, CVE-2021-34523.	2021-07-14	5.2	CVE-2021-33768 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33776, CVE-2021-33777.	2021-07-14	6.8	CVE-2021-33778 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33776, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33775 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33776 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33776, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33777 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33775, CVE-2021-33776, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-31947 MISC
microsoft -- open_enclave_software_development_kit	Open Enclave SDK Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33767 MISC
microsoft -- power_bi_report_server	Power BI Remote Code Execution Vulnerability	2021-07-14	6.8	CVE-2021-31984 MISC
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33773, CVE-2021-34445, CVE-2021-34456.	2021-07-14	4.6	CVE-2021-33761 MISC
microsoft -- windows_10	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33772, CVE-2021-34490.	2021-07-14	5	CVE-2021-31183 MISC
microsoft -- windows_10	Windows Desktop Bridge Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33759 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34460, CVE-2021-34510, CVE-2021-34512, CVE-2021-34513.	2021-07-14	4.6	CVE-2021-33751 MISC
microsoft -- windows_10	Windows Projected File System Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33743 MISC
microsoft -- windows_10	Windows Event Tracing Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33774 MISC
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-34445, CVE-2021-34456.	2021-07-14	4.6	CVE-2021-33773 MISC
microsoft -- windows_10	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33784 MISC
microsoft -- windows_10	Windows Authenticode Spoofing Vulnerability	2021-07-14	4.3	CVE-2021-33782 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33750, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33752 MISC
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33755.	2021-07-14	4	CVE-2021-33758 MISC
microsoft -- windows_10	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-31183, CVE-2021-34490.	2021-07-14	5	CVE-2021-33772 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33750, CVE-2021-33752.	2021-07-14	6.8	CVE-2021-33756 MISC
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33758.	2021-07-14	5	CVE-2021-33755 MISC
microsoft -- windows_10	Windows SMB Information Disclosure Vulnerability	2021-07-14	4	CVE-2021-33783 MISC
microsoft -- windows_10	Windows AF_UNIX Socket Provider Denial of Service Vulnerability	2021-07-14	5	CVE-2021-33785 MISC
microsoft -- windows_10	Azure AD Security Feature Bypass Vulnerability	2021-07-14	5.5	CVE-2021-33781 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33750, CVE-2021-33752, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33749 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33752, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33750 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33754, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6.5	CVE-2021-33780 MISC
microsoft -- windows_server_2008	Windows Key Distribution Center Information Disclosure Vulnerability	2021-07-14	4.3	CVE-2021-33764 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33754, CVE-2021-33780, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6.5	CVE-2021-33746 MISC
microsoft -- windows_server_2008	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-34442, CVE-2021-34444, CVE-2021-34499.	2021-07-14	4	CVE-2021-33745 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33780, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6	CVE-2021-33754 MISC
microsoft -- windows_server_2016	Windows ADFS Security Feature Bypass Vulnerability	2021-07-14	5.5	CVE-2021-33779 MISC
mikrotik -- routeros	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference). NOTE: this is different from CVE-2020-20253 and CVE-2020-20254. All four vulnerabilities in the /nova/bin/lcdstat process are discussed in the CVE-2020-20250 github.com/cq674350529 reference.	2021-07-13	4	CVE-2020-20250 MISC MISC
mikrotik -- routeros	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-07-13	4	CVE-2020-20252 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mitre -- caldera	A command injection vulnerability in the sandcat plugin of Caldera 2.3.1 and earlier allows authenticated attackers to execute any command or service.	2021-07-12	6.5	CVE-2020-19907 MISC
moddable -- moddable	Issue was discovered in the fxParserTree function in moddable, allows attackers to cause denial of service via a crafted payload. Fixed in commit 723816ab9b52f807180c99fc69c7d08cf6c6bd61.	2021-07-13	5	CVE-2020-22882 MISC
nextcloud -- nextcloud	Nextcloud Android Client is the Android client for Nextcloud. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.16.1, the Nextcloud Android client skipped a step that involved the client checking if a private key belonged to a previously downloaded public certificate. If the Nextcloud instance served a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor. The vulnerability is patched in version 3.16.1. As a workaround, do not add additional end-to-end encrypted devices to a user account.	2021-07-12	5	CVE-2021-32727 CONFIRM MISC MISC MISC
nextcloud -- nextcloud_mail	Nextcloud Mail is a mail app for Nextcloud. In versions prior to 1.9.6, the Nextcloud Mail application does not, by default, render images in emails to not leak the read state. The privacy filter failed to filter images with a `background-image` CSS attribute. Note that the images were still passed through the Nextcloud image proxy, and thus there was no IP leakage. The issue was patched in version 1.9.6 and 1.10.0. No workarounds are known to exist.	2021-07-12	4	CVE-2021-32707 MISC MISC CONFIRM
nextcloud -- nextcloud_server	Nextcloud Text is a collaborative document editing application that uses Markdown. A cross-site scripting vulnerability is present in versions prior to 19.0.13, 20.0.11, and 21.0.3. The Nextcloud Text application shipped with Nextcloud server used a `text/html` Content-Type when serving files to users. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, use a browser that has support for Content-Security-Policy.	2021-07-12	4.3	CVE-2021-32733 MISC MISC CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the shareinfo endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32703 CONFIRM MISC MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public DAV endpoint. This may have allowed an attacker to enumerate potentially valid share tokens or credentials. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32705 MISC MISC CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, filenames where not escaped by default in controllers using `DownloadResponse`. When a user-supplied filename was passed unsanitized into a `DownloadResponse`, this could be used to trick users into downloading malicious files with a benign file extension. This would show in UI behaviours where Nextcloud applications would display a benign file extension (e.g. JPEG), but the file will actually be downloaded with an executable file extension. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. Administrators of Nextcloud instances do not have a workaround available, but developers of Nextcloud apps may manually escape the file name before passing it into `DownloadResponse`.	2021-07-12	6.8	CVE-2021-32679 CONFIRM MISC MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, ratelimits are not applied to OCS API responses. This affects any OCS API controller (`OCSController`) using the `@BruteForceProtection` annotation. Risk depends on the installed applications on the Nextcloud Server, but could range from bypassing authentication ratelimits or spamming other Nextcloud users. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. No workarounds aside from upgrading are known to exist.	2021-07-12	5	CVE-2021-32678 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public share link mount endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32741 MISC MISC CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, the Nextcloud Text application shipped with Nextcloud Server returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, one may disable the Nextcloud Text application in Nextcloud Server app settings.	2021-07-12	5	CVE-2021-32734 CONFIRM MISC MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, default share permissions were not being respected for federated reshares of files and folders. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32725 CONFIRM MISC MISC
nextcloud -- talk	Nextcloud Talk is a fully on-premises audio/video and chat communication service. In versions prior to 11.2.2, if a user was able to reuse an earlier used username, they could get access to any chat message sent to the previous user with this username. The issue was patched in versions 11.2.2 and 11.3.0. As a workaround, don't allow users to choose usernames themselves. This is the default behaviour of Nextcloud, but some user providers may allow doing so.	2021-07-12	4	CVE-2021-32689 MISC MISC MISC CONFIRM MISC
nodejs -- node.js	Node.js before 16.4.1, 14.17.2, 12.22.2 is vulnerable to an out-of-bounds read when uv__idna_toascii() is used to convert strings to ASCII. The pointer p is read and increased without checking whether it is beyond pe, with the latter holding a pointer to the end of the buffer. This can lead to information disclosures or crashes. This function can be triggered via uv_getaddrinfo().	2021-07-12	6.4	CVE-2021-22918 MISC MISC
nodejs -- node.js	Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory allows an attacker to perform two different escalation attacks: PATH and DLL hijacking.	2021-07-12	4.4	CVE-2021-22921 MISC MISC
openvpn -- openvpn	OpenVPN 3 Core Library version 3.6 and 3.6.1 allows a man-in-the-middle attacker to bypass the certificate authentication by issuing an unrelated server certificate using the same hostname found in the verify-x509-name option in a client configuration.	2021-07-12	5.8	CVE-2021-3547 MISC MISC
panasonic -- fpwin_pro	Panasonic FPWIN Pro, all Versions 7.5.1.1 and prior, allows an attacker to craft a project file specifying a URI that causes the XML parser to access the URI and embed the contents, which may allow the attacker to disclose information that is accessible in the context of the user executing software.	2021-07-09	4.3	CVE-2021-32972 MISC
pbootcms -- pbootcms	Incorrect Access Control vulnerability in PbootCMS 2.0.6 via the list parameter in the update function in upgradecontroller.php.	2021-07-09	4	CVE-2020-22535 MISC
pfsense -- pfsense	Netgate pfSense Community Edition 2.4.4 - p2 (arm64) is affected by: Cross Site Scripting (XSS). The impact is: Session Hijacking, Information Leakage (local). The component is: pfSense Dashboard, Work-on-LAN Service configuration. The attack vector is: Inject the malicious JavaScript code in Description text box or parameter.	2021-07-12	4.3	CVE-2020-19203 MISC MISC
plugin-planet -- prismatic	The Prismatic WordPress plugin before 2.8 does not escape the 'tab' GET parameter before outputting it back in an attribute, leading to a reflected Cross-Site Scripting issue which will be executed in the context of a logged in administrator	2021-07-12	4.3	CVE-2021-24409 CONFIRM
pluginus -- wordpress_meta_data_and_taxonomies_filter	Cross-site request forgery (CSRF) vulnerability in WordPress Meta Data Filter & Taxonomies Filter versions prior to v.1.2.8 and versions prior to v.2.2.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-14	6.8	CVE-2021-20781 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
putty -- putty	PuTTY through 0.75 proceeds with establishing an SSH session even if it has never sent a substantive authentication response. This makes it easier for an attacker-controlled SSH server to present a later spoofed authentication prompt (that the attacker can use to capture credential data, and use that data for purposes that are undesired by the client user).	2021-07-09	5.8	CVE-2021-36367 MISC MISC
qualcomm -- apq8009_firmware	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	5	CVE-2021-1955 CONFIRM
qualcomm -- apq8053_firmware	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-07-13	5	CVE-2021-1970 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-07-13	5	CVE-2021-1907 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1964 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1943 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1954 CONFIRM
qualcomm -- apq8053_firmware	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1945 CONFIRM
qualcomm -- aqt1000_firmware	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1953 CONFIRM
qualcomm -- aqt1000_firmware	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1938 CONFIRM
qualcomm -- ar7420_firmware	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1887 CONFIRM
quickjs_project -- quickjs	Buffer Overflow vulnerability in quickjs.c in QuickJS, allows remote attackers to cause denial of service. This issue is resolved in the 2020-07-05 release.	2021-07-13	5	CVE-2020-22876 MISC
redhat -- keycloak	A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.	2021-07-09	5	CVE-2021-3637 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
restsharp -- restsharp	RestSharp < 106.11.8-alpha.0.13 uses a regular expression which is vulnerable to Regular Expression Denial of Service (ReDoS) when converting strings into DateTimes. If a server responds with a malicious string, the client using RestSharp will be stuck processing it for an exceedingly long time. Thus the remote server can trigger Denial of Service.	2021-07-12	5	CVE-2021-27293 MISC MISC
retty -- retty	Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 uses a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app.	2021-07-14	5	CVE-2021-20748 MISC MISC
retty -- retty	Improper authorization in handler for custom URL scheme vulnerability in Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	2021-07-14	4.3	CVE-2021-20747 MISC MISC
rockwellautomation -- micrologix_1100_firmware	Rockwell Automation MicroLogix 1100, all versions, allows a remote, unauthenticated attacker sending specially crafted commands to cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault whenever the controller is switched to RUN mode.	2021-07-09	5	CVE-2021-33012 MISC
salonbookingsystem -- salon_booking_system	The Salon booking system WordPress plugin before 6.3.1 does not properly sanitise and escape the First Name field when booking an appointment, allowing low privilege users such as subscriber to set JavaScript in them, leading to a Stored Cross-Site Scripting (XSS) vulnerability. The Payload will then be triggered when an admin visits the "Calendar" page and the malicious script is executed in the admin context.	2021-07-12	4.3	CVE-2021-24429 CONFIRM
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes out of bounds write and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	2021-07-14	4.3	CVE-2021-33681 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes buffer overflow and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	2021-07-14	4.3	CVE-2021-33680 MISC MISC
sap -- businessobjects_web_intelligence	Under certain conditions, SAP Business Objects Web Intelligence (BI Launchpad) versions - 420, 430, allows an attacker to access jsp source code, through SDK calls, of Analytical Reporting bundle, a part of the frontend application, which would otherwise be restricted.	2021-07-14	4	CVE-2021-33667 MISC MISC
sap -- customer_relationship_managemen	A missing authority check in SAP CRM, versions - 700, 701, 702, 712, 713, 714, could be leveraged by an attacker with high privileges to compromise confidentiality, integrity, or availability of the system.	2021-07-14	6.5	CVE-2021-33676 MISC MISC
sap -- netweaver_abap	SAP NetWeaver ABAP Server and ABAP Platform, versions - 700, 702, 730, 731, 804, 740, 750, 784, expose functions to external which can lead to information disclosure.	2021-07-14	5	CVE-2021-33677 MISC MISC
sap -- netweaver_application_server_java	When user with insufficient privileges tries to access any application in SAP NetWeaver Administrator (Administrator applications), version - 7.50, no security audit log is created. Therefore, security audit log Integrity is impacted.	2021-07-14	4	CVE-2021-33689 MISC MISC
sap -- netweaver_application_server_java	SAP NetWeaver AS for Java (Http Service Monitoring Filter), versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send multiple HTTP requests with different method types thereby crashing the filter and making the HTTP server unavailable to other legitimate users leading to denial of service vulnerability.	2021-07-14	5	CVE-2021-33670 MISC MISC
sap -- netweaver_application_server_java	SAP NetWeaver AS JAVA (Enterprise Portal), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50 reveals sensitive information in one of their HTTP requests, an attacker can use this in conjunction with other attacks such as XSS to steal this information.	2021-07-14	4	CVE-2021-33687 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- netweaver_guided_procedures	SAP NetWeaver Guided Procedures (Administration Workset), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. The impact of missing authorization could result to abuse of functionality restricted to a particular user group, and could allow unauthorized users to read, modify or delete restricted data.	2021-07-14	6.5	CVE-2021-33671 MISC MISC
segment -- is-email	A ReDoS (regular expression denial of service) flaw was found in the Segment is-email package before 1.0.1 for Node.js. An attacker that is able to provide crafted input to the isEmail(input) function may cause an application to consume an excessive amount of CPU.	2021-07-14	5	CVE-2021-36716 MISC CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13404)	2021-07-13	6.8	CVE-2021-34319 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13442)	2021-07-13	6.8	CVE-2021-34331 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13430)	2021-07-13	6.8	CVE-2021-34330 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427)	2021-07-13	6.8	CVE-2021-34329 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13199)	2021-07-13	4.3	CVE-2021-34304 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422)	2021-07-13	6.8	CVE-2021-34326 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13420)	2021-07-13	6.8	CVE-2021-34324 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13419)	2021-07-13	6.8	CVE-2021-34323 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The DL180CoolType.dll library in affected applications lacks proper validation of user-supplied data when parsing PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13380)	2021-07-13	6.8	CVE-2021-34316 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423)	2021-07-13	6.8	CVE-2021-34327 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13343)	2021-07-13	4.3	CVE-2021-34307 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13356)	2021-07-13	6.8	CVE-2021-34315 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13355)	2021-07-13	6.8	CVE-2021-34314 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13354)	2021-07-13	6.8	CVE-2021-34313 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13353)	2021-07-13	6.8	CVE-2021-34312 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Mono_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13352)	2021-07-13	6.8	CVE-2021-34311 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13192)	2021-07-13	4.3	CVE-2021-34299 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13197)	2021-07-13	4.3	CVE-2021-34302 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13198)	2021-07-13	4.3	CVE-2021-34303 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13403)	2021-07-13	6.8	CVE-2021-34318 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424)	2021-07-13	6.8	CVE-2021-34328 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCX files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13402)	2021-07-13	6.8	CVE-2021-34317 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12956)	2021-07-13	6.8	CVE-2021-34291 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13057)	2021-07-13	6.8	CVE-2021-34296 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12959)	2021-07-13	6.8	CVE-2021-34292 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The VisDraw.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13414)	2021-07-13	4.3	CVE-2021-34321 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13406)	2021-07-13	4.3	CVE-2021-34320 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13421)	2021-07-13	4.3	CVE-2021-34325 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in an infinite loop condition that leads to denial of service condition. An attacker could leverage this vulnerability to consume excessive resources. (CNVD-C-2021-79300)	2021-07-13	4.3	CVE-2021-34332 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in double free of an allocated buffer that leads to a crash. An attacker could leverage this vulnerability to cause denial of service condition. (CNVD-C-2021-79295)	2021-07-13	4.3	CVE-2021-34333 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13351)	2021-07-13	6.8	CVE-2021-34310 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13344)	2021-07-13	4.3	CVE-2021-34308 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The JPEG2K_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13416)	2021-07-13	4.3	CVE-2021-34322 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13350)	2021-07-13	6.8	CVE-2021-34309 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13024)	2021-07-13	6.8	CVE-2021-34295 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13342)	2021-07-13	6.8	CVE-2021-34306 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13340)	2021-07-13	6.8	CVE-2021-34305 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13020)	2021-07-13	6.8	CVE-2021-34293 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13196)	2021-07-13	6.8	CVE-2021-34301 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13194)	2021-07-13	6.8	CVE-2021-34300 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13060)	2021-07-13	6.8	CVE-2021-34298 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13023	2021-07-13	6.8	CVE-2021-34294 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13059)	2021-07-13	6.8	CVE-2021-34297 CONFIRM
sonicwall -- switch	Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling LLDP Protocol allows an attacker to cause a system instability or potentially read sensitive information from the memory locations.	2021-07-09	6.8	CVE-2021-20024 CONFIRM
stormshield -- endpoint_security	Stormshield Endpoint Security Evolution 2.0.0 through 2.0.2 does not accomplish the intended defense against local administrators who can replace the Visual C++ runtime DLLs (in %WINDIR%\system32) with malicious ones.	2021-07-13	4.6	CVE-2021-35957 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows deleting some resources not currently in use by any security policy by leveraging access to a computer having the administration console installed.	2021-07-13	4.3	CVE-2021-31225 MISC MISC
tipsandtricks-hq -- software_license_manager	Cross-site request forgery (CSRF) vulnerability in Software License Manager versions prior to 4.4.6 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-14	6.8	CVE-2021-20782 MISC MISC MISC
vmware -- cloud_foundation	SFCB (Small Footprint CIM Broker) as used in ESXi has an authentication bypass vulnerability. A malicious actor with network access to port 5989 on ESXi may exploit this issue to bypass SFCB authentication by sending a specially crafted request.	2021-07-13	6.8	CVE-2021-21994 MISC
vmware -- cloud_foundation	OpenSLP as used in ESXi has a denial-of-service vulnerability due a heap out-of-bounds read issue. A malicious actor with network access to port 427 on ESXi may be able to trigger a heap out-of-bounds read in OpenSLP service resulting in a denial-of-service condition.	2021-07-13	5	CVE-2021-21995 MISC
vmware -- thinapp	VMware Thinapp version 5.x prior to 5.2.10 contain a DLL hijacking vulnerability due to insecure loading of DLLs. A malicious actor with non-administrative privileges may exploit this vulnerability to elevate privileges to administrator level on the Windows operating system having VMware ThinApp installed on it.	2021-07-13	6.9	CVE-2021-22000 MISC FULLDISC
voidtools -- everything	HTTP header injection vulnerability in Everything all versions except the Lite version may allow a remote attacker to inject an arbitrary script or alter the website that uses the product via unspecified vectors.	2021-07-14	5.8	CVE-2021-20784 MISC MISC MISC
wayang-cms_project -- wayang-cms	A SQL injection vulnerability in wy_controlls/wy_side_visitor.php of Wayang-CMS v1.0 allows attackers to obtain sensitive database information.	2021-07-14	5	CVE-2020-29147 MISC
wayang-cms_project -- wayang-cms	A cross site scripting (XSS) vulnerability in index.php of Wayang-CMS v1.0 allows attackers to execute arbitrary web scripts or HTML via a constructed payload created by adding the X-Forwarded-For field to the header.	2021-07-14	4.3	CVE-2020-29146 MISC
wire -- wire	Wire is a collaboration platform. wire-ios-transport handles authentication of requests, network failures, and retries for the iOS implementation of Wire. In the 3.82 version of the iOS application, a new web socket implementation was introduced for users running iOS 13 or higher. This new websocket implementation is not configured to enforce certificate pinning when available. Certificate pinning for the new websocket is enforced in version 3.84 or above.	2021-07-13	4	CVE-2021-32755 CONFIRM
xen-orchestra -- xo-server	Xen Orchestra (with xo-web through 5.80.0 and xo-server through 5.84.0) mishandles authorization, as demonstrated by modified WebSocket resourceSet.getAll data is which the attacker changes the permission field from none to admin. The attacker gains access to data sets such as VMs, Backups, Audit, Users, and Groups.	2021-07-12	4	CVE-2021-36383 MISC
xml\ -- \	It was discovered that the XML::Atom Perl module before version 0.39 did not disable external entities when parsing XML from potentially untrusted sources. This may allow attackers to gain read access to otherwise protected resources, depending on how the library is used.	2021-07-09	5	CVE-2012-1102 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xmlsoft -- libxml2	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.	2021-07-09	4	CVE-2021-3541 MISC
yop-poll -- yop_poll	In the YOP Poll WordPress plugin before 6.2.8, when a pool is created with the options "Allow other answers", "Display other answers in the result list" and "Show results", it can lead to Stored Cross-Site Scripting issues as the 'Other' answer is not sanitised before being output in the page. The execution of the XSS payload depends on the 'Show results' option selected, which could be before or after sending the vote for example.	2021-07-12	4.3	CVE-2021-24454 MISC CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
admincolumns -- admin_columns	The Admin Columns WordPress plugin Free before 4.3.2 and Pro before 5.5.2 allowed to configure individual columns for tables. Each column had a type. The type "Custom Field" allowed to choose an arbitrary database column to display in the table. There was no escaping applied to the contents of "Custom Field" columns.	2021-07-12	3.5	CVE-2021-24365 CONFIRM MISC
blackcat-cms -- blackcat_cms	A stored cross site scripting (XSS) vulnerability in the 'Add Page' feature of BlackCat CMS 1.3.6 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	2021-07-09	3.5	CVE-2020-25877 MISC MISC
blackcat-cms -- blackcat_cms	A stored cross site scripting (XSS) vulnerability in the 'Admin-Tools' feature of BlackCat CMS 1.3.6 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payloads entered into the 'Output Filters' and 'Droplets' modules.	2021-07-09	3.5	CVE-2020-25878 MISC MISC
boldgrid -- w3_total_cache	The W3 Total Cache WordPress plugin before 2.1.3 did not sanitise or escape some of its CDN settings, allowing high privilege users to use JavaScript in them, which will be output in the page, leading to an authenticated Stored Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24427 MISC CONFIRM
codologic -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Manage Users' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Username' parameter.	2021-07-09	3.5	CVE-2020-25879 MISC MISC
codologic -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Smileys' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Smiley Code' parameter.	2021-07-09	3.5	CVE-2020-25875 MISC MISC
codologic -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Pages' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Page Title' parameter.	2021-07-09	3.5	CVE-2020-25876 MISC MISC
cszcms -- csz_cms	A cross site scripting vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New Pages' field under the 'Pages Content' module.	2021-07-09	3.5	CVE-2020-25391 MISC
cszcms -- csz_cms	A cross site scripting (XSS) vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New Article' field under the 'Article' plugin.	2021-07-09	3.5	CVE-2020-25392 MISC
dotcms -- dotcms	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/containers of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	2021-07-09	3.5	CVE-2021-35360 MISC
dotcms -- dotcms	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/links of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	2021-07-09	3.5	CVE-2021-35361 MISC
dotcms -- dotcms	A stored cross site scripting (XSS) vulnerability in dotAdmin/#/c/c_Images of dotCMS 21.05.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' and 'Filename' parameters.	2021-07-09	3.5	CVE-2021-35358 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
element-it -- http_commander	A Cross-site scripting (XSS) vulnerability in the "View in Browser" feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to inject arbitrary web script or HTML via a crafted SVG image.	2021-07-14	3.5	CVE-2021-33212 MISC MISC
emarketdegisn -- request_a_quote	The Request a Quote WordPress plugin before 2.3.4 did not sanitise and escape some of its quote fields when adding/editing a quote as admin, leading to Stored Cross-Site scripting issues when the quote is output in the 'All Quotes" table.	2021-07-12	3.5	CVE-2021-24420 CONFIRM
esri -- arcgis_server	A stored Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server Services Directory version 10.8.1 and below may allow a remote authenticated attacker to pass and store malicious strings in the ArcGIS Services Directory.	2021-07-11	3.5	CVE-2021-29105 CONFIRM
eyecix -- jobsearch_wp_job_board	The WP JobSearch WordPress plugin before 1.7.4 did not sanitise or escape multiple of its parameters from the my-resume page before outputting them in the page, allowing low privilege users to use JavaScript payloads in them and leading to a Stored Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24421 CONFIRM MISC
fetchdesigns -- sign-up_sheets	The Sign-up Sheets WordPress plugin before 1.0.14 did not sanitise or escape some of its fields when creating a new sheet, allowing high privilege users to add JavaScript in them, leading to a Stored Cross-Site Scripting issue. The payloads will be triggered when viewing the 'All Sheets' page in the admin dashboard	2021-07-12	3.5	CVE-2021-24440 CONFIRM
flowdroid_project -- flowdroid	FlowDroid is a data flow analysis tool. FlowDroid versions prior to 2.9.0 contained an XML external entity (XXE) vulnerability that allowed an attacker who had control over the source/sink definition file in XML format to read files from external locations. In order for this to occur, the XML-based format for sources and sinks had to be used and the attacker had to able control the source/sink definition file. The vulnerability was patched in version 2.9.0. As a workaround, do not allow untrusted entities to control the source/sink definition file.	2021-07-12	3.5	CVE-2021-32754 CONFIRM
google -- android	In generateFileInfo of BluetoothOppSendFileInfo.java, there is a possible way to share private files over Bluetooth due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179910660	2021-07-14	1.9	CVE-2021-0604 MISC
halo -- halo	Cross Sie Scripting (XSS) vulnerability in Halo 0.4.3 via CommentAuthorUrl.	2021-07-12	3.5	CVE-2020-18982 MISC
huawei -- mate_20_firmware	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1), 9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1).	2021-07-13	2.1	CVE-2021-22440 MISC
huawei -- p30_firmware	The Bluetooth function of some Huawei smartphones has a DoS vulnerability. Attackers can install third-party apps to send specific broadcasts, causing the Bluetooth module to crash. This vulnerability is successfully exploited to cause the Bluetooth function to become abnormal. Affected product versions include: HUAWEI P30 10.0.0.195(C432E22R2P5), 10.0.0.200(C00E85R2P11), 10.0.0.200(C461E6R3P1), 10.0.0.201(C10E7R5P1), 10.0.0.201(C185E4R7P1), 10.0.0.206(C605E19R1P3), 10.0.0.209(C636E6R3P4), 10.0.0.210(C635E3R2P4), and versions earlier than 10.1.0.165(C01E165R2P11).	2021-07-13	2.1	CVE-2021-22399 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195035.	2021-07-13	3.5	CVE-2021-20364 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195357.	2021-07-13	3.5	CVE-2021-20368 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195037.	2021-07-13	3.5	CVE-2021-20366 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195036.	2021-07-13	3.5	CVE-2021-20365 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195034.	2021-07-13	3.5	CVE-2021-20363 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195033.	2021-07-13	3.5	CVE-2021-20362 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195032.	2021-07-13	3.5	CVE-2021-20361 XF CONFIRM
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204262.	2021-07-12	3.5	CVE-2021-29804 XF CONFIRM
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204263.	2021-07-12	3.5	CVE-2021-29805 CONFIRM XF
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204164.	2021-07-12	3.5	CVE-2021-29803 CONFIRM XF
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204349.	2021-07-12	3.5	CVE-2021-29822 CONFIRM XF
icinga -- icinga	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Between versions 2.3.0 and 2.8.2, the `doc` module of Icinga Web 2 allows to view documentation directly in the UI. It must be enabled manually by an administrator and users need explicit access permission to use it. Then, by visiting a certain route, it is possible to gain access to arbitrary files readable by the web-server user. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, an administrator may disable the `doc` module or revoke permission to use it from all users.	2021-07-12	3.5	CVE-2021-32746 MISC CONFIRM MISC MISC
kaseya -- vsa	Cross Site Scripting (XSS) exists in Kaseya VSA before 9.5.7.	2021-07-09	3.5	CVE-2021-30119 MISC
microsoft -- windows_10	Media Foundation Information Disclosure Vulnerability	2021-07-14	2.1	CVE-2021-33760 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Remote Access Connection Manager Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-34454, CVE-2021-34457.	2021-07-14	2.1	CVE-2021-33763 MISC
microsoft -- windows_10	Windows Installer Spoofing Vulnerability	2021-07-14	2.1	CVE-2021-33765 MISC
microsoft -- windows_10	Windows InstallService Elevation of Privilege Vulnerability	2021-07-14	3.6	CVE-2021-31961 MISC
mozilo -- mozilocms	A stored cross site scripting (XSS) vulnerability in moziloCMS 2.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Content" parameter.	2021-07-09	3.5	CVE-2020-25394 MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions priot to 19.0.13, 20.0.11, and 21.0.3, Nextcloud Server audit logging functionality wasn't properly logging events for the unsetting of a share expiration date. This event is supposed to be logged. This issue is patched in versions 19.0.13, 20.0.11, and 21.0.3.	2021-07-12	2.1	CVE-2021-32680 CONFIRM MISC MISC
pfsense -- pfsense	A Stored Cross-Site Scripting (XSS) vulnerability was found in status_filter_reload.php, a page in the pfSense software WebGUI, on Netgate pfSense version 2.4.4-p2 and earlier. The page did not encode output from the filter reload process, and a stored XSS was possible via the descr (description) parameter on NAT rules.	2021-07-12	3.5	CVE-2020-19201 MISC MISC MISC
plugin-planet -- prismatic	The Prismatic WordPress plugin before 2.8 does not sanitise or validate some of its shortcode parameters, allowing users with a role as low as Contributor to set Cross-Site payload in them. A post made by a contributor would still have to be approved by an admin to have the XSS trigger able in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability.	2021-07-12	3.5	CVE-2021-24408 CONFIRM
prothemedesign -- browser_screenshots	The Browser Screenshots WordPress plugin before 1.7.6 allowed authenticated users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks as the image_class parameter of the browser-shot shortcode was not escaped.	2021-07-12	3.5	CVE-2021-24439 CONFIRM
publiccms -- publiccms	Cross Site Scripting (XSS) vulnerability in PublicCMS 4.0 to get an admin cookie when the Administrator reviews submit case.	2021-07-09	3.5	CVE-2020-21333 MISC
qualcomm -- apq8009_firmware	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1901 CONFIRM
qualcomm -- apq8009_firmware	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1897 CONFIRM
qualcomm -- apq8009_firmware	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1898 CONFIRM
qualcomm -- apq8009w_firmware	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1899 CONFIRM
qualcomm -- aqt1000_firmware	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity	2021-07-13	3.3	CVE-2021-1896 CONFIRM
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Users Access Groups' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	3.5	CVE-2020-35986 MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Entities List' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	3.5	CVE-2020-35987 MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Users Alerts' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	2021-07-09	3.5	CVE-2020-35984 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Global Lists" feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	3.5	CVE-2020-35985 MISC
sap -- lumira_server	SAP Lumira Server version 2.4 does not sufficiently encode user controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. This would allow an attacker with basic level privileges to store a malicious script on SAP Lumira Server. The execution of the script content, by a victim registered on SAP Lumira Server, could compromise the confidentiality and integrity of SAP Lumira content.	2021-07-14	3.5	CVE-2021-33682 MISC MISC
smooth_scroll_page_up\/down_buttons_project -- smooth_scroll_page_up\/down_buttons	The Smooth Scroll Page Up/Down Buttons WordPress plugin through 1.4 does not properly sanitise and validate its psb_positioning settings, allowing high privilege users such as admin to set an XSS payload in it, which will be executed in all pages of the blog	2021-07-12	3.5	CVE-2021-24418 CONFIRM MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows duplicating an existing security policy by leveraging access of a user having read-only access to security policies.	2021-07-13	2.9	CVE-2021-31224 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows modifying security policies by leveraging access of a user having read-only access to security policies.	2021-07-13	2.3	CVE-2021-31220 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows reading some parts of a security policy by leveraging access to a computer having the administration console installed.	2021-07-13	2.9	CVE-2021-31223 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows updating some parts of a security policy by leveraging access to a computer having the administration console installed.	2021-07-13	2.9	CVE-2021-31222 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows deleting some parts of a security policy by leveraging access to a computer having the administration console installed.	2021-07-13	2.9	CVE-2021-31221 MISC MISC
web-dorado -- backup-wd	The Backup by 10Web â€“ Backup and Restore Plugin WordPress plugin through 1.0.20 does not sanitise or escape the tab parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24426 MISC CONFIRM
webfactoryltd -- wp_reset	The WP Reset â€“ Most Advanced WordPress Reset Tool WordPress plugin before 1.90 did not sanitise or escape its extra_data parameter when creating a snapshot via the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24424 CONFIRM MISC
wp_youtube_lyte_project -- wp_youtube_lyte	The WP YouTube Lyte WordPress plugin before 1.7.16 did not sanitise or escape its lyte_yt_api_key and lyte_notification settings before outputting them back in the page, allowing high privilege users to set XSS payload on them and leading to stored Cross-Site Scripting issues.	2021-07-12	3.5	CVE-2021-24419 CONFIRM MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1password_connect -- 1password_connect	1Password Connect server before 1.2 is missing validation checks, permitting users to create Secrets Automation access tokens that can be used to perform privilege escalation. Malicious users authorized to create Secrets Automation access tokens can create tokens that have access beyond what the user is authorized to access, but limited to the existing authorizations of the Secret Automation the token is created in.	2021-07-16	not yet calculated	CVE-2021-36758 MISC
MdeModulePkg -- MdeModulePkg	Insufficient input validation in MdeModulePkg in EDKII may allow an unauthenticated user to potentially enable escalation of privilege, denial of service and/or information disclosure via physical access.	2021-07-14	not yet calculated	CVE-2019-11098 MISC
acronis -- true_image	Acronis True Image through 2021 on macOS allows local privilege escalation from admin to root due to insecure folder permissions.	2021-07-15	not yet calculated	CVE-2020-25593 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acronis -- true_image	Acronis True Image 2019 update 1 through 2021 update 1 on macOS allows local privilege escalation due to an insecure XPC service configuration.	2021-07-15	not yet calculated	CVE-2020-25736 MISC MISC
acronis -- true_image_2019	Acronis True Image for Mac before 2021 Update 4 allowed local privilege escalation due to insecure folder permissions.	2021-07-15	not yet calculated	CVE-2020-15496 MISC MISC
acronis -- true_image_2019	Acronis True Image 2019 update 1 through 2020 on macOS allows local privilege escalation due to an insecure XPC service configuration.	2021-07-15	not yet calculated	CVE-2020-15495 MISC MISC
advantech -- r-seenet	A local file inclusion (LFI) vulnerability exists in the options.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). A specially crafted HTTP request can lead to arbitrary PHP code execution. An attacker can send a crafted HTTP request to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21804 MISC
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	not yet calculated	CVE-2021-21801 MISC
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	not yet calculated	CVE-2021-21802 MISC
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	not yet calculated	CVE-2021-21803 MISC
advantech -- r-seenet	Cross-site scripting vulnerabilities exist in the ssh_form.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). If a user visits a specially crafted URL, it can lead to arbitrary JavaScript code execution in the context of the targeted user's browser. An attacker can provide a crafted URL to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21800 MISC
advantech -- r-seenet	Cross-site scripting vulnerabilities exist in the telnet_form.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). If a user visits a specially crafted URL, it can lead to arbitrary JavaScript code execution in the context of the targeted user's browser. An attacker can provide a crafted URL to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21799 MISC
apache -- commons_compress	When reading a specially crafted ZIP archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' zip package.	2021-07-13	not yet calculated	CVE-2021-36090 MISC MISC MLIST MLIST MLIST MLIST MLIST MLIST
apache -- commons_compress	When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	2021-07-13	not yet calculated	CVE-2021-35515 MISC MISC MLIST MLIST
apache -- commons_compress	When reading a specially crafted TAR archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' tar package.	2021-07-13	not yet calculated	CVE-2021-35517 MISC MISC MLIST MLIST MLIST MLIST MLIST
apache -- commons_compress	When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	2021-07-13	not yet calculated	CVE-2021-35516 MISC MISC MLIST MLIST
apache -- mina_sshd	A vulnerability in sshd-core of Apache Mina SSHD allows an attacker to overflow the server causing an OutOfMemory error. This issue affects the SFTP and port forwarding features of Apache Mina SSHD version 2.0.0 and later versions. It was addressed in Apache Mina SSHD 2.7.0	2021-07-12	not yet calculated	CVE-2021-30129 CONFIRM MLIST MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- tomcat	A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.	2021-07-12	not yet calculated	CVE-2021-30640 MISC
booking_core -- ultimate_booking_system_booking_core	Cross Site Scripting (XSS) vulnerability in Booking Core - Ultimate Booking System Booking Core 1.7.0 via the (1) "About Yourself" section under the “My Profile” page, " (2) “Hotel Policy” field under the “Hotel Details” page, (3) “Pricing code” and “name” fields under the “Manage Tour” page, and (4) all the labels under the “Menu” section.	2021-07-14	not yet calculated	CVE-2020-25444 MISC
broadcom -- bcm4352_and_bcm43684	A vulnerability exists in Broadcom BCM4352 and BCM43684 chips. Any wireless router using BCM4352 and BCM43684 will be affected, such as ASUS AX6100. An attacker may cause a Denial of Service (DoS) to any device connected to BCM4352 or BCM43684 routers via an association or reassociation frame.	2021-07-14	not yet calculated	CVE-2021-34174 MISC MISC
cartadis -- gespage	Cartadis Gespage through 8.2.1 allows Directory Traversal in gespage/doDownloadData and gespage/webapp/doDownloadData.	2021-07-12	not yet calculated	CVE-2021-33807 MISC CONFIRM MISC
centreon -- platform	An issue was discovered in Centreon-Web in Centreon Platform 20.10.0. A SQL injection vulnerability in "Configuration > Users > Contacts / Users" allows remote authenticated users to execute arbitrary SQL commands via the Additional Information parameters.	2021-07-16	not yet calculated	CVE-2021-28053 MISC MISC MISC
centreon -- platform	An issue was discovered in Centreon-Web in Centreon Platform 20.10.0. A Stored Cross-Site Scripting (XSS) issue in "Configuration > Hosts" allows remote authenticated users to inject arbitrary web script or HTML via the Alias parameter.	2021-07-16	not yet calculated	CVE-2021-28054 MISC MISC MISC
chatwoot -- chatwoot	chatwoot is vulnerable to Inefficient Regular Expression Complexity	2021-07-16	not yet calculated	CVE-2021-3649 MISC CONFIRM
cisco -- adaptive_security_appliance	A vulnerability in the software cryptography module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker or an unauthenticated attacker in a man-in-the-middle position to cause an unexpected reload of the device that results in a denial of service (DoS) condition. The vulnerability is due to a logic error in how the software cryptography module handles specific types of decryption errors. An attacker could exploit this vulnerability by sending malicious packets over an established IPsec connection. A successful exploit could cause the device to crash, forcing it to reload. Important: Successful exploitation of this vulnerability would not cause a compromise of any encrypted data. Note: This vulnerability affects only Cisco ASA Software Release 9.16.1 and Cisco FTD Software Release 7.0.0.	2021-07-16	not yet calculated	CVE-2021-1422 CISCO
d-link -- dap-1330_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the Cookie HTTP header. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-12028.	2021-07-15	not yet calculated	CVE-2021-34830 MISC
d-link -- dap-1330_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the SOAPAction HTTP header. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-12029.	2021-07-15	not yet calculated	CVE-2021-34827 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d-link -- dap-1330_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the SOAPAction HTTP header. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-12066.	2021-07-15	not yet calculated	CVE-2021-34828 MISC
d-link -- dap-1330_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1330 1.13B01 BETA routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the HNAP_AUTH HTTP header. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-12065.	2021-07-15	not yet calculated	CVE-2021-34829 MISC
d-link -- dir-3040	A hard-coded password vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to a denial of service. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21818 MISC
d-link -- dir-3040	An information disclosure vulnerability exists in the Syslog functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to the disclosure of sensitive information. An attacker can send an HTTP request to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21816 MISC
d-link -- dir-3040	An information disclosure vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to the disclosure of sensitive information. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21817 MISC
d-link -- dir-3040	A code execution vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21819 MISC
d-link -- dir-3040	A hard-coded password vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	not yet calculated	CVE-2021-21820 MISC
dell -- emc_avamar_server	Dell EMC Avamar Server versions 7.4.1, 7.5.0, 7.5.1, 18.2 and 19.1 and Dell EMC Integrated Data Protection Appliance (IDPA) versions 2.0, 2.1, 2.2, 2.3 and 2.4. contain an XML External Entity(XXE) Injection vulnerability. A remote unauthenticated malicious user could potentially exploit this vulnerability to cause Denial of Service or information exposure by supplying specially crafted document type definitions (DTDs) in an XML request.	2021-07-16	not yet calculated	CVE-2019-3752 MISC
dell -- wyse_management_suite	Wyse Management Suite versions 3.2 and earlier contain an absolute path traversal vulnerability. A remote authenticated malicious user could exploit this vulnerability in order to read arbitrary files on the system.	2021-07-15	not yet calculated	CVE-2021-21586 MISC
dell -- wyse_management_suite	Dell Wyse Management Suite versions 3.2 and earlier contain a full path disclosure vulnerability. A local unauthenticated attacker could exploit this vulnerability in order to obtain the path of files and folders.	2021-07-15	not yet calculated	CVE-2021-21587 MISC
depstech -- wifi_digital_microscope_3	DEPSTECH WiFi Digital Microscope 3 allows remote attackers to change the SSID and password, and demand a ransom payment from the rightful device owner, because there is no way to reset to Factory Default settings.	2021-07-15	not yet calculated	CVE-2020-12734 MISC MISC
depstech -- wifi_digital_microscope_3	Certain Shenzhen PENGLIXIN components on DEPSTECH WiFi Digital Microscope 3, as used by Shekar Endoscope, allow a TELNET connection with the molinkadmin password for the molink account.	2021-07-15	not yet calculated	CVE-2020-12733 MISC MISC
depstech -- wifi_digital_microscope_3	DEPSTECH WiFi Digital Microscope 3 has a default SSID of Jetion_xxxxxxxx with a password of 12345678.	2021-07-15	not yet calculated	CVE-2020-12732 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
discourse -- discourse	Discourse is an open-source discussion platform. In Discourse versions 2.7.5 and prior, parsing and rendering of YouTube Oneboxes can be susceptible to XSS attacks. This vulnerability only affects sites which have modified or disabled Discourse's default Content Security Policy. The issue is patched in `stable` version 2.7.6, `beta` version 2.8.0.beta3, and `tests-passed` version 2.8.0.beta3. As a workaround, ensure that the Content Security Policy is enabled, and has not been modified in a way which would make it more vulnerable to XSS attacks.	2021-07-15	not yet calculated	CVE-2021-32764 CONFIRM
dr.id -- door_access_control_and_personnel_attendance_management_system	Dr. ID Door Access Control and Personnel Attendance Management system uses the hard-code admin default credentials that allows remote attackers to access the system through the default password and obtain the highest permission.	2021-07-16	not yet calculated	CVE-2021-35961 MISC MISC
dr.id -- door_access_control_and_personnel_attendance_management_system	Specific page parameters in Dr. ID Door Access Control and Personnel Attendance Management system does not filter special characters. Remote attackers can apply Path Traversal means to download credential files from the system without permission.	2021-07-16	not yet calculated	CVE-2021-35962 MISC MISC
eclipse -- jetty	For Eclipse Jetty versions 9.4.37-9.4.42, 10.0.1-10.0.5 & 11.0.1-11.0.5, URIs can be crafted using some encoded characters to access the content of the WEB-INF directory and/or bypass some security constraints. This is a variation of the vulnerability reported in CVE-2021-28164/GHSA-v7ff-8wcx-gmc5.	2021-07-15	not yet calculated	CVE-2021-34429 CONFIRM
ecostructure -- control_expert	Insufficiently Protected Credentials vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause unauthorized access to a project file protected by a password when this file is shared with untrusted sources. An attacker may bypass the password protection and be able to view and modify a project file.	2021-07-14	not yet calculated	CVE-2021-22780 MISC
ecostructure -- control_expert	Insufficiently Protected Credentials vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause a leak of SMTP credential used for mailbox authentication when an attacker can access a project file.	2021-07-14	not yet calculated	CVE-2021-22781 MISC
ecostructure -- control_expert	Authentication Bypass by Spoofing vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Control Expert V15.0 SP1, EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), SCADAPack RemoteConnect for x70 (all versions), Modicon M580 CPU (all versions - part numbers BMEP* and BMEH*), Modicon M340 CPU (all versions - part numbers BMXP34*), that could cause unauthorized access in read and write mode to the controller by spoofing the Modbus communication between the engineering software and the controller.	2021-07-14	not yet calculated	CVE-2021-22779 MISC
ecostructure -- control_expert	Insufficiently Protected Credentials vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause protected derived function blocks to be read or modified by unauthorized users when accessing a project file.	2021-07-14	not yet calculated	CVE-2021-22778 MISC
ecostructure -- control_expert	Missing Encryption of Sensitive Data vulnerability exists in EcoStruxure Control Expert (all versions prior to V15.0 SP1, including all versions of Unity Pro), EcoStruxure Process Expert (all versions, including all versions of EcoStruxure Hybrid DCS), and SCADAPack RemoteConnect for x70, all versions, that could cause an information leak allowing disclosure of network and process information, credentials or intellectual property when an attacker can access a project file.	2021-07-14	not yet calculated	CVE-2021-22782 MISC
ectouch -- ectouch	SQL Injection Vulnerability in ECTouch v2 via the integral_min parameter in index.php.	2021-07-14	not yet calculated	CVE-2020-18144 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elfinder.net.core -- elfinder.net.core	This affects the package elFinder.Net.Core from 0 and before 1.2.4. The user-controlled file name is not properly sanitized before it is used to create a file system path.	2021-07-14	not yet calculated	CVE-2021-23407 MISC MISC MISC
espressif -- esp32	An attacker can cause a Denial of Service and kernel panic in v4.2 and earlier versions of Espressif esp32 via a malformed beacon csa frame. The device requires a reboot to recover.	2021-07-14	not yet calculated	CVE-2021-34173 MISC MISC
fail2ban -- fail2ban	fail2ban is a daemon to ban hosts that cause multiple authentication errors. In versions 0.9.7 and prior, 0.10.0 through 0.10.6, and 0.11.0 through 0.11.2, there is a vulnerability that leads to possible remote code execution in the mailing action mail-whois. Command `mail` from mailutils package used in mail actions like `mail-whois` can execute command if unescaped sequences (`\n~`) are available in "foreign" input (for instance in whois output). To exploit the vulnerability, an attacker would need to insert malicious characters into the response sent by the whois server, either via a MITM attack or by taking over a whois server. The issue is patched in versions 0.10.7 and 0.11.3. As a workaround, one may avoid the usage of action `mail-whois` or patch the vulnerability manually.	2021-07-16	not yet calculated	CVE-2021-32749 MISC MISC CONFIRM
falco -- falco	Falco through 0.28.1 has a Time-of-check Time-of-use (TOCTOU) Race Condition. Issue is fixed in Falco versions >= 0.29.1.	2021-07-15	not yet calculated	CVE-2021-33505 MISC
fossil -- fossil	Fossil before 2.14.2 and 2.15.x before 2.15.2 often skips the hostname check during TLS certificate validation.	2021-07-12	not yet calculated	CVE-2021-36377 MISC
froala -- wysiwyg	Froala WYSIWYG Editor 3.2.6-1 is affected by XSS due to a namespace confusion during parsing.	2021-07-16	not yet calculated	CVE-2021-28114 MISC MISC MISC
fsso -- collector	An improper authentication vulnerability in FSSO Collector version 5.0.295 and below may allow an unauthenticated user to bypass a FSSO firewall policy and access the protected network via sending specifically crafted UDP login notification packets.	2021-07-12	not yet calculated	CVE-2021-26088 CONFIRM
gatsby -- gatsby	Gatsby is a framework for building websites. The gatsby-source-wordpress plugin prior to versions 4.0.8 and 5.9.2 leaks .htaccess HTTP Basic Authentication variables into the app.js bundle during build-time. Users who are not initializing basic authentication credentials in the gatsby-config.js are not affected. A patch has been introduced in gatsby-source-wordpress@4.0.8 and gatsby-source-wordpress@5.9.2 which mitigates the issue by filtering all variables specified in the `auth: { }` section. Users that depend on this functionality are advised to upgrade to the latest release of gatsby-source-wordpress, run `gatsby clean` followed by a `gatsby build`. One may manually edit the app.js file post-build as a workaround.	2021-07-15	not yet calculated	CVE-2021-32770 CONFIRM
github -- enterprise_server	A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.3 and was fixed in 3.1.3, 3.0.11, and 2.22.17. This vulnerability was reported via the GitHub Bug Bounty program.	2021-07-14	not yet calculated	CVE-2021-22867 MISC MISC MISC
go -- go	The crypto/tls package of Go through 1.16.5 does not properly assert that the type of public key in an X.509 certificate matches the expected type when doing a RSA based key exchange, allowing a malicious TLS server to cause a TLS client to panic.	2021-07-15	not yet calculated	CVE-2021-34558 MISC MISC MISC
google -- android	In isRealSnapshot of TaskThumbnailView.java, there is possible data exposure due to a missing permission check. This could lead to local information disclosure from locked profiles with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168802517References: N/A	2021-07-14	not yet calculated	CVE-2021-0654 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hashicorp -- consul	HashiCorp Consul before 1.10.1 (and Consul Enterprise) has Missing SSL Certificate Validation. xds does not ensure that the Subject Alternative Name of an upstream is validated.	2021-07-17	not yet calculated	CVE-2021-32574 MISC CONFIRM
hashicorp -- consul	In HashiCorp Consul before 1.10.1 (and Consul Enterprise), xds can generate a situation where a single L7 deny intention (with a default deny policy) results in an allow action.	2021-07-17	not yet calculated	CVE-2021-36213 MISC CONFIRM
hitachi -- abb_power_grids_esoms	Password autocomplete vulnerability in the web application password field of Hitachi ABB Power Grids eSOMS allows attacker to gain access to user credentials that are stored by the browser. This issue affects: Hitachi ABB Power Grids eSOMS version 6.3 and prior versions.	2021-07-14	not yet calculated	CVE-2021-35527 CONFIRM
ibm -- infosphere_data_republican	IBM InfoSphere Data Replication 11.4 and IBM InfoSphere Change Data Capture for z/OS 10.2.1, under certain configurations, could allow a user to bypass authentication mechanisms using an empty password string. IBM X-Force ID: 189834	2021-07-16	not yet calculated	CVE-2020-4821 CONFIRM CONFIRM XF
ibm -- infosphere_master_data_management_server	IBM InfoSphere Master Data Management Server 11.6 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 186324.	2021-07-16	not yet calculated	CVE-2020-4675 CONFIRM XF
ibm -- qradar_siem	IBM QRadar SIEM 7.3 and 7.4 uses less secure methods for protecting data in transit between hosts when encrypt host connections is not enabled as well as data at rest. IBM X-Force ID: 192539.	2021-07-16	not yet calculated	CVE-2020-4980 CONFIRM XF
ibm -- secure_external_authentication_server	IBM Secure External Authentication Server 2.4.3.2, 6.0.1, 6.0.2 and IBM Secure Proxy 3.4.3.2, 6.0.1, 6.0.2 could allow a remote user to consume resources causing a denial of service due to a resource leak.	2021-07-15	not yet calculated	CVE-2021-29725 CONFIRM XF CONFIRM
ibm -- secure_external_authentication_server	IBM Secure External Authentication Server 6.0.2 and IBM Secure Proxy 6.0.2 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 201777.	2021-07-15	not yet calculated	CVE-2021-29749 XF CONFIRM CONFIRM
ibm -- security_access_amanger	IBM Security Access Manager 9.0 and IBM Security Verify Access Docker 10.0.0 stores user credentials in plain clear text which can be read by an unauthorized user.	2021-07-15	not yet calculated	CVE-2021-20439 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 198660	2021-07-15	not yet calculated	CVE-2021-20523 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 198814	2021-07-15	not yet calculated	CVE-2021-20534 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 198300.	2021-07-15	not yet calculated	CVE-2021-20511 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198661.	2021-07-15	not yet calculated	CVE-2021-20524 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could reveal highly sensitive information to a local privileged user. IBM X-Force ID: 197980.	2021-07-15	not yet calculated	CVE-2021-20500 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 197969	2021-07-15	not yet calculated	CVE-2021-20497 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow an authenticated user to bypass input due to improper input validation. IBM X-Force ID: 197966.	2021-07-15	not yet calculated	CVE-2021-20496 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 198813	2021-07-15	not yet calculated	CVE-2021-20533 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 197973	2021-07-15	not yet calculated	CVE-2021-20499 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow a user to impersonate another user on the system. IBM X-Force ID: 201483.	2021-07-15	not yet calculated	CVE-2021-29742 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 reveals version information in HTTP requets that could be used in further attacks against the system. IBM X-Force ID: 197972.	2021-07-15	not yet calculated	CVE-2021-20498 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 198299	2021-07-15	not yet calculated	CVE-2021-20510 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 could allow a remote priviled user to upload arbitrary files with a dangerous file type that could be excuted by an user. IBM X-Force ID: 200600.	2021-07-15	not yet calculated	CVE-2021-29699 XF CONFIRM
ibm -- security_verify_access_docker	IBM Security Verify Access Docker 10.0.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID:198918	2021-07-15	not yet calculated	CVE-2021-20537 XF CONFIRM
icinga -- icinga	Icinga is a monitoring system which checks the availability of network resources, notifies users of outages, and generates performance data for reporting. In versions prior to 2.11.10 and from version 2.12.0 through version 2.12.4, some of the Icinga 2 features that require credentials for external services expose those credentials through the API to authenticated API users with read permissions for the corresponding object types. IdoMysqlConnection and IdoPgsqlConnection (every released version) exposes the password of the user used to connect to the database. IcingaDB (added in 2.12.0) exposes the password used to connect to the Redis server. ElasticsearchWriter (added in 2.8.0)exposes the password used to connect to the Elasticsearch server. An attacker who obtains these credentials can impersonate Icinga to these services and add, modify and delete information there. If credentials with more permissions are in use, this increases the impact accordingly. Starting with the 2.11.10 and 2.12.5 releases, these passwords are no longer exposed via the API. As a workaround, API user permissions can be restricted to not allow querying of any affected objects, either by explicitly listing only the required object types for object query permissions, or by applying a filter rule.	2021-07-15	not yet calculated	CVE-2021-32743 MISC CONFIRM
icinga -- icinga	Icinga is a monitoring system which checks the availability of network resources, notifies users of outages, and generates performance data for reporting. From version 2.4.0 through version 2.12.4, a vulnerability exists that may allow privilege escalation for authenticated API users. With a read-ony user's credentials, an attacker can view most attributes of all config objects including `ticket_salt` of `ApiListener`. This salt is enough to compute a ticket for every possible common name (CN). A ticket, the master node's certificate, and a self-signed certificate are enough to successfully request the desired certificate from Icinga. That certificate may in turn be used to steal an endpoint or API user's identity. Versions 2.12.5 and 2.11.10 both contain a fix the vulnerability. As a workaround, one may either specify queryable types explicitly or filter out ApiListener objects.	2021-07-15	not yet calculated	CVE-2021-32739 MISC CONFIRM
idrive -- remotepc	iDrive RemotePC before 4.0.1 on Linux allows denial of service. A remote and unauthenticated attacker can disconnect a valid user session by connecting to an ephemeral port.	2021-07-15	not yet calculated	CVE-2021-34691 MISC MISC
idrive -- remotepc	iDrive RemotePC before 7.6.48 on Windows allows information disclosure. A locally authenticated attacker can read an encrypted version of the system's Personal Key in world-readable %PROGRAMDATA% log files. The encryption is done using a hard-coded static key and is therefore reversible by an attacker.	2021-07-15	not yet calculated	CVE-2021-34688 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idrive -- remotepc	iDrive RemotePC before 7.6.48 on Windows allows information disclosure. A locally authenticated attacker can read the system's Personal Key in world-readable %PROGRAMDATA% log files.	2021-07-15	not yet calculated	CVE-2021-34689 MISC MISC
idrive -- remotepc	iDrive RemotePC before 7.6.48 on Windows allows authentication bypass. A remote and unauthenticated attacker can bypass cloud authentication to connect and control a system via TCP port 5970 and 5980.	2021-07-15	not yet calculated	CVE-2021-34690 MISC MISC
idrive -- remotepc	iDrive RemotePC before 7.6.48 on Windows allows privilege escalation. A local and low-privileged user can force RemotePC to execute an attacker-controlled executable with SYSTEM privileges.	2021-07-15	not yet calculated	CVE-2021-34692 MISC MISC
idrive -- remotepc	iDrive RemotePC before 7.6.48 on Windows allows information disclosure. A man in the middle can recover a system's Personal Key when a client attempts to make a LAN connection. The Personal Key is transmitted over the network while only being encrypted via a substitution cipher.	2021-07-15	not yet calculated	CVE-2021-34687 MISC MISC
intel -- bssa_dft	Insecure default variable initialization for the Intel BSSA DFT feature may allow a privileged user to potentially enable an escalation of privilege via local access.	2021-07-14	not yet calculated	CVE-2021-0144 MISC
intelliants -- subrion_cms	SQL Injection vulnerability in Subrion CMS v4.2.1 in the search page if a website uses a PDO connection.	2021-07-14	not yet calculated	CVE-2020-18155 MISC
jamf -- pro	Jamf Pro before 10.30.1 allows for an unvalidated URL redirect vulnerability affecting Jamf Pro customers who host their environments on-premises. An attacker may craft a URL that appears to be for a customer's Jamf Pro instance, but when clicked will forward a user to an arbitrary URL that may be malicious. This is tracked via Jamf with the following ID: PI-009822	2021-07-12	not yet calculated	CVE-2021-35037 MISC MISC
jasper -- image_coding_toolkit	A Divide-by-zero vulnerability exists in JasPer Image Coding Toolkit 2.0 in jasper/src/libjasper/jpc/jpc_enc.c	2021-07-15	not yet calculated	CVE-2021-27845 MISC
jfif_encode -- jfif_encode	A global buffer overflow vulnerability in jfif_encode at jfif.c:701 of ffjpeg through 2020-06-22 allows attackers to cause a Denial of Service (DOS) via a crafted jpeg file.	2021-07-15	not yet calculated	CVE-2020-23705 MISC
jt -- utilities	A vulnerability has been identified in JT Utilities (All versions < V13.0.2.0). When parsing specially crafted JT files, a race condition could cause an object to be released before being operated on, leading to NULL pointer deference condition and causing the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.	2021-07-13	not yet calculated	CVE-2021-33715 CONFIRM
jt -- utilities	A vulnerability has been identified in JT Utilities (All versions < V13.0.2.0). When parsing specially crafted JT files, a missing check for the validity of an iterator leads to NULL pointer deference condition, causing the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.	2021-07-13	not yet calculated	CVE-2021-33714 CONFIRM
jt -- utilities	A vulnerability has been identified in JT Utilities (All versions < V13.0.2.0). When parsing specially crafted JT files, a hash function is called with an incorrect argument leading the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.	2021-07-13	not yet calculated	CVE-2021-33713 CONFIRM
juniper_networks -- contrail_cloud	Juniper Networks Contrail Cloud (CC) releases prior to 13.6.0 have RabbitMQ service enabled by default with hardcoded credentials. The messaging services of RabbitMQ are used when coordinating operations and status information among Contrail services. An attacker with access to an administrative service for RabbitMQ (e.g. GUI), can use these hardcoded credentials to cause a Denial of Service (DoS) or have access to unspecified sensitive system information. This issue affects the Juniper Networks Contrail Cloud releases on versions prior to 13.6.0.	2021-07-15	not yet calculated	CVE-2021-0279 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in the handling of exceptional conditions in Juniper Networks Junos OS Evolved (EVO) allows an attacker to send specially crafted packets to the device, causing the Advanced Forwarding Toolkit manager (evo-aftmand-bt or evo-aftmand-zx) process to crash and restart, impacting all traffic going through the FPC, resulting in a Denial of Service (DoS). Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Following messages will be logged prior to the crash: Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:32710470974358 label:1089551617 for session:18 probe:35 Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:19241453497049 label:1089551617 for session:18 probe:37 Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:19241453497049 label:1089551617 for session:18 probe:44 Feb 2 10:14:39 fpc0 evo-aftmand-bt[16263]: [Error] Nexthop: Failed to get fwd nexthop for nexthop:32710470974358 label:1089551617 for session:18 probe:47 Feb 2 10:14:39 fpc0 audit[16263]: ANOM_ABEND auid=4294967295 uid=0 gid=0 ses=4294967295 pid=16263 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=11 Feb 2 10:14:39 fpc0 kernel: audit: type=1701 audit(1612260879.272:17): auid=4294967295 uid=0 gid=0 ses=4294967295 pid=16263 comm="EvoAftManBt-mai" exe="/usr/sbin/evo-aftmand-bt" sig=1 This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1 versions prior to 21.1R2-EVO.	2021-07-15	not yet calculated	CVE-2021-0286 CONFIRM
juniper_networks -- junos_os	An Improper Input Validation vulnerability in J-Web of Juniper Networks Junos OS allows a locally authenticated attacker to escalate their privileges to root over the target device. junos:18.3R3-S5 junos:18.4R3-S9 junos:19.1R3-S6 junos:19.3R2-S6 junos:19.3R3-S3 junos:19.4R1-S4 junos:19.4R3-S4 junos:20.1R2-S2 junos:20.1R3 junos:20.2R3-S1 junos:20.3X75-D20 junos:20.3X75-D30 junos:20.4R2-S1 junos:20.4R3 junos:21.1R1-S1 junos:21.1R2 junos:21.2R1 junos:21.3R1 This issue affects: Juniper Networks Junos OS 19.3 versions 19.3R1 and above prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.	2021-07-15	not yet calculated	CVE-2021-0278 CONFIRM
juniper_networks -- junos_os	On Juniper Networks Junos OS devices with Multipath or add-path feature enabled, processing a specific BGP UPDATE can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued receipt and processing of this UPDATE message will create a sustained Denial of Service (DoS) condition. This BGP UPDATE message can propagate to other BGP peers with vulnerable Junos versions on which Multipath or add-path feature is enabled, and cause RPD to crash and restart. This issue affects both IBGP and EBGP deployments in IPv4 or IPv6 network. Junos OS devices that do not have the BGP Multipath or add-path feature enabled are not affected by this issue. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S18; 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S3;	2021-07-15	not yet calculated	CVE-2021-0282 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	Improper Handling of Exceptional Conditions in Ethernet interface frame processing of Juniper Networks Junos OS allows an attacker to send specially crafted frames over the local Ethernet segment, causing the interface to go into a down state, resulting in a Denial of Service (DoS) condition. The interface does not recover on its own and the FPC must be reset manually. Continued receipt and processing of these frames will create a sustained Denial of Service (DoS) condition. This issue is platform-specific and affects the following platforms and line cards: * MPC7E/8E/9E and MPC10E on MX240, MX480, MX960, MX2008, MX2010, and MX2020 * MX204, MX10003, MX10008, MX10016 * EX9200, EX9251 * SRX4600 No other products or platforms are affected by this vulnerability. An indication of this issue occurring can be seen in the system log messages, as shown below: user@host> show log messages | match "Failed to complete DFE tuning" fpc4 smic_phy_dfe_tuning_state: et-4/1/6 - Failed to complete DFE tuning (count 3) and interface will be in a permanently down state: user@host> show interfaces et-4/1/6 terse Interface Admin Link Proto Local Remote et-4/1/6 up down et-4/1/6.0 up down aenet --> ae101.0 This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S7 on MX Series; 17.1R1 and later versions prior to 17.2R3-S3 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S11, 17.4R3-S1 on MX Series, SRX4600; 18.1 versions prior to 18.1R3-S10 on MX Series, EX9200 Series, SRX4600; 18.2 versions prior to 18.2R3-S3 on MX Series, EX9200 Series, SRX4600; 18.3 versions prior to 18.3R3-S1 on MX Series, EX9200 Series, SRX4600; 18.4 versions prior to 18.4R2-S3, 18.4R3 on MX Series, EX9200 Series, SRX4600; 19.1 versions prior to 19.1R2-S1, 19.1R3 on MX Series, EX9200 Series, SRX4600; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series, EX9200 Series, SRX4600; 19.3 versions prior to 19.3R2 on MX Series, EX9200 Series, SRX4600. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1.	2021-07-15	not yet calculated	CVE-2021-0290 CONFIRM
juniper_networks -- junos_os	When user-defined ARP Policer is configured and applied on one or more Aggregated Ethernet (AE) interface units, a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability between the Device Control Daemon (DCD) and firewall process (dfwd) daemons of Juniper Networks Junos OS allows an attacker to bypass the user-defined ARP Policer. In this particular case the User ARP policer is replaced with default ARP policer. To review the desired ARP Policers and actual state one can run the command "show interfaces <> extensive" and review the output. See further details below. An example output is: show interfaces extensive | match policer Policer: Input: __default_arp_policer__ <<< incorrect if user ARP Policer was applied on an AE interface and the default ARP Policer is displayed Policer: Input: jtac-arp-ae5.317-inet-arp <<< correct if user ARP Policer was applied on an AE interface For all platforms, except SRX Series: This issue affects Juniper Networks Junos OS: All versions 5.6R1 and all later versions prior to 18.4 versions prior to 18.4R2-S9, 18.4R3-S9 with the exception of 15.1 versions 15.1R7-S10 and later versions; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S2; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2; This issue does not affect Juniper Networks Junos OS versions prior to 5.6R1. On SRX Series this issue affects Juniper Networks Junos OS: 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.4 versions prior to 19.4R3-S4; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S2; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2. This issue does not affect 18.4 versions prior to 18.4R1 on SRX Series. This issue does not affect Junos OS Evolved.	2021-07-15	not yet calculated	CVE-2021-0289 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in the Distance Vector Multicast Routing Protocol (DVMRP) of Juniper Networks Junos OS on the QFX10K Series switches allows an attacker to trigger a packet forwarding loop, leading to a partial Denial of Service (DoS). The issue is caused by DVMRP packets looping on a multi-homed Ethernet Segment Identifier (ESI) when VXLAN is configured. DVMRP packets received on a multi-homed ESI are sent to the peer, and then incorrectly forwarded out the same ESI, violating the split horizon rule. This issue only affects QFX10K Series switches, including the QFX10002, QFX10008, and QFX10016. Other products and platforms are unaffected by this vulnerability. This issue affects Juniper Networks Junos OS on QFX10K Series: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 version 18.2R1 and later versions; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S9, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2.	2021-07-15	not yet calculated	CVE-2021-0295 CONFIRM
juniper_networks -- junos_os	An Exposure of System Data vulnerability in Juniper Networks Junos OS and Junos OS Evolved, where a sensitive system-level resource is not being sufficiently protected, allows a network-based unauthenticated attacker to send specific traffic which partially reaches this resource. A high rate of specific traffic may lead to a partial Denial of Service (DoS) as the CPU utilization of the RE is significantly increased. The SNMP Agent Extensibility (agentx) process should only be listening to TCP port 705 on the internal routing instance. External connections destined to port 705 should not be allowed. This issue affects: Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R2. Juniper Networks Junos OS Evolved versions prior to 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 13.2R1.	2021-07-15	not yet calculated	CVE-2021-0291 CONFIRM
juniper_networks -- junos_os	A vulnerability in Juniper Networks Junos OS caused by Missing Release of Memory after Effective Lifetime leads to a memory leak each time the CLI command 'show system connections extensive' is executed. The amount of memory leaked on each execution depends on the number of TCP connections from and to the system. Repeated execution will cause more memory to leak and eventually daemons that need to allocate additionally memory and ultimately the kernel to crash, which will result in traffic loss. Continued execution of this command will cause a sustained Denial of Service (DoS) condition. An administrator can use the following CLI command to monitor for increase in memory consumption of the netstat process, if it exists: user@junos> show system processes extensive | match "username|netstat" PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 21181 root 100 0 5458M 4913M CPU3 2 0:59 97.27% netstat The following log message might be observed if this issue happens: kernel: %KERN-3: pid 21181 (netstat), uid 0, was killed: out of swap space This issue affects Juniper Networks Junos OS 18.2 versions prior to 18.2R2-S8, 18.2R3-S7. 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2; This issue does not affect Juniper Networks Junos OS versions prior to 18.2R1.	2021-07-15	not yet calculated	CVE-2021-0293 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in Juniper Networks Junos OS, which only affects the release 18.4R2-S5, where a function is inconsistently implemented on Juniper Networks Junos QFX5000 Series and EX4600 Series, and if "storm-control enhanced" is configured, can lead to the enhanced storm control filter group not be installed. It will cause storm control not to work hence allowing an attacker to cause high CPU usage or packet loss issues by sending a large amount of broadcast or unknown unicast packets arriving the device. This issue affects Juniper Networks QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, EX4600, and EX4650, and QFX5100 with QFX 5e Series image installed. QFX5130 and QFX5220 are not affected from this issue. This issue affects Juniper Networks Junos OS 18.4R2-S5 on QFX5000 Series and EX4600 Series. No other product or platform is affected by this vulnerability.	2021-07-15	not yet calculated	CVE-2021-0294 CONFIRM
juniper_networks -- junos_os	An Out-of-bounds Read vulnerability in the processing of specially crafted LLDP frames by the Layer 2 Control Protocol Daemon (l2cpd) of Juniper Networks Junos OS and Junos OS Evolved may allow an attacker to cause a Denial of Service (DoS), or may lead to remote code execution (RCE). Continued receipt and processing of these frames, sent from the local broadcast domain, will repeatedly crash the l2cpd process and sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S18; 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved versions prior to 20.4R2-EVO.	2021-07-15	not yet calculated	CVE-2021-0277 CONFIRM
juniper_networks -- junos_os	A vulnerability in the processing of specific MPLS packets in Juniper Networks Junos OS on MX Series and EX9200 Series devices with Trio-based MPCs (Modular Port Concentrators) may cause FPC to crash and lead to a Denial of Service (DoS) condition. Continued receipt of this packet will sustain the Denial of Service (DoS) condition. This issue only affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). This issue affects Juniper Networks Junos OS on MX Series, EX9200 Series: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2;	2021-07-15	not yet calculated	CVE-2021-0288 CONFIRM
juniper_networks -- junos_os	In a Segment Routing ISIS (SR-ISIS)/MPLS environment, on Juniper Networks Junos OS and Junos OS Evolved devices, configured with ISIS Flexible Algorithm for Segment Routing and sensor-based statistics, a flap of a ISIS link in the network, can lead to a routing process daemon (RPD) crash and restart, causing a Denial of Service (DoS). Continued link flaps will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 19.4 versions prior to 19.4R1-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R2; Juniper Networks Junos OS Evolved: 20.3-EVO versions prior to 20.3R2-EVO; 20.4-EVO versions prior to 20.4R2-EVO. This issue does not affect: Juniper Networks Junos OS releases prior to 19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO.	2021-07-15	not yet calculated	CVE-2021-0287 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On Juniper Networks Junos OS devices configured with BGP origin validation using Resource Public Key Infrastructure (RPKI) receipt of a specific packet from the RPKI cache server may cause routing process daemon (RPD) to crash and restart, creating a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R2-S2-EVO.	2021-07-15	not yet calculated	CVE-2021-0281 CONFIRM
juniper_networks -- junos_os	An uncontrolled resource consumption vulnerability in Juniper Networks Junos OS on QFX5000 Series and EX4600 Series switches allows an attacker sending large amounts of legitimate traffic destined to the device to cause Interchassis Control Protocol (ICCP) interruptions, leading to an unstable control connection between the Multi-Chassis Link Aggregation Group (MC-LAG) nodes which can in turn lead to traffic loss. Continued receipt of this amount of traffic will create a sustained Denial of Service (DoS) condition. An indication that the system could be impacted by this issue is the following log message: "DDOS_PROTOCOL_VIOLATION_SET: Warning: Host-bound traffic for protocol/exception LOCALNH:aggregate exceeded its allowed bandwidth at fpc <fpc number> for <n> times, started at <timestamp>" This issue affects Juniper Networks Junos OS on QFX5000 Series and EX4600 Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S5; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R2-S8, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2.	2021-07-15	not yet calculated	CVE-2021-0285 CONFIRM
juniper_networks -- junos_os	A buffer overflow vulnerability in the TCP/IP stack of Juniper Networks Junos OS allows an attacker to send specific sequences of packets to the device thereby causing a Denial of Service (DoS). By repeatedly sending these sequences of packets to the device, an attacker can sustain the Denial of Service (DoS) condition. The device will abnormally shut down as a result of these sent packets. A potential indicator of compromise will be the following message in the log files: "eventd[13955]: SYSTEM_ABNORMAL_SHUTDOWN: System abnormally shut down" These issue are only triggered by traffic destined to the device. Transit traffic will not trigger these issues. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S19; 15.1 versions prior to 15.1R7-S10; 16.1 version 16.1R1 and later versions; 16.2 version 16.2R1 and later versions; 17.1 version 17.1R1 and later versions; 17.2 version 17.2R1 and later versions; 17.3 version 17.3R1 and later versions; 18.1 versions prior to 18.1R3-S13; 18.2 version 18.2R1 and later versions; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior ot 18.4R3-S9; 19.1 versions prior to 19.1R3-S6; 19.2 versions prior to 19.2R3-S3; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R1-S4, 19.4R3-S5; 20.1 versions prior to 20.1R2-S2, 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2; 21.2 versions prior to 21.2R2.	2021-07-15	not yet calculated	CVE-2021-0283 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	Due to an Improper Initialization vulnerability in Juniper Networks Junos OS on PTX platforms and QFX10K Series with Paradise (PE) chipset-based line cards, ddos-protection configuration changes made from the CLI will not take effect as expected beyond the default DDoS (Distributed Denial of Service) settings in the Packet Forwarding Engine (PFE). This may cause BFD sessions to flap when a high rate of specific packets are received. Flapping of BFD sessions in turn may impact routing protocols and network stability, leading to a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects only the following platforms with Paradise (PE) chipset-based line cards: PTX1000, PTX3000 (NextGen), PTX5000, PTX10008, PTX10016 Series and QFX10002 Series. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R3-S5 on PTX Series, QFX10K Series; 18.2 versions prior to 18.2R3-S8 on PTX Series, QFX10K Series; 18.3 versions prior to 18.3R3-S5 on PTX Series, QFX10K Series; 18.4 versions prior to 18.4R2-S8 on PTX Series, QFX10K Series; 19.1 versions prior to 19.1R3-S5 on PTX Series, QFX10K Series; 19.2 versions prior to 19.2R3-S2 on PTX Series, QFX10K Series; 19.3 versions prior to 19.3R3-S2 on PTX Series, QFX10K Series; 19.4 versions prior to 19.4R3-S2 on PTX Series, QFX10K Series; 20.1 versions prior to 20.1R3 on PTX Series, QFX10K Series; 20.2 versions prior to 20.2R2-S3, 20.2R3 on PTX Series, QFX10K Series; 20.3 versions prior to 20.3R2 on PTX Series, QFX10K Series; 20.4 versions prior to 20.4R2 on PTX Series, QFX10K Series.	2021-07-15	not yet calculated	CVE-2021-0280 CONFIRM
juniper_networks -- junos_os	An Uncontrolled Resource Consumption vulnerability in the ARP daemon (arpd) and Network Discovery Protocol (ndp) process of Juniper Networks Junos OS Evolved allows a malicious attacker on the local network to consume memory resources, ultimately resulting in a Denial of Service (DoS) condition. Link-layer functions such as IPv4 and/or IPv6 address resolution may be impacted, leading to traffic loss. The processes do not recover on their own and must be manually restarted. Changes in memory usage can be monitored using the following shell commands (header shown for clarity): user@router:/var/log# ps aux | grep arpd USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 31418 59.0 0.7 *5702564* 247952 ? xxx /usr/sbin/arpd --app-name arpd -l object_select --shared-objects-mode 3 user@router:/var/log# ps aux | grep arpd USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 31418 49.1 1.0 *5813156* 351184 ? xxx /usr/sbin/arpd --app-name arpd -l object_select --shared-objects-mode 3 Memory usage can be monitored for the ndp process in a similar fashion: user@router:/var/log# ps aux | grep ndp USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 14935 0.0 0.1 *5614052* 27256 ? Ssl Jun15 0:17 /usr/sbin/ndp -l no_tab_chk,object_select --app-name ndp --shared-obje user@router:/var/log# ps aux | grep ndp USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 14935 0.0 0.1 *5725164* 27256 ? Ssl Jun15 0:17 /usr/sbin/ndp -l no_tab_chk,object_select --app-name ndp --shared-obje This issue affects Juniper Networks Junos OS Evolved: 19.4 versions prior to 19.4R2-S3-EVO; 20.1 versions prior to 20.1R2-S4-EVO; all versions of 20.2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.4R2-EVO.	2021-07-15	not yet calculated	CVE-2021-0292 CONFIRM
juniper_networks -- sbr_carrier	A stack-based Buffer Overflow vulnerability in Juniper Networks SBR Carrier with EAP (Extensible Authentication Protocol) authentication configured, allows an attacker sending specific packets causing the radius daemon to crash resulting with a Denial of Service (DoS) or leading to remote code execution (RCE). By continuously sending this specific packets, an attacker can repeatedly crash the radius daemon, causing a sustained Denial of Service (DoS). This issue affects Juniper Networks SBR Carrier: 8.4.1 versions prior to 8.4.1R19; 8.5.0 versions prior to 8.5.0R10; 8.6.0 versions prior to 8.6.0R4.	2021-07-15	not yet calculated	CVE-2021-0276 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- multiple_products	Some Lenovo Notebook, ThinkPad, and Lenovo Desktop systems have BIOS modules unprotected by Intel Boot Guard that could allow an attacker with physical access the ability to write to the SPI flash storage.	2021-07-16	not yet calculated	CVE-2021-3453 MISC
lenovo -- notebook	A vulnerability was reported on some Lenovo Notebook systems that could allow an attacker with physical access to elevate privileges under certain conditions during a BIOS update performed by Lenovo Vantage.	2021-07-16	not yet calculated	CVE-2021-3614 MISC
lenovo -- pcmanager	A DLL search path vulnerability was reported in Lenovo PCManager, prior to version 3.0.500.5102, that could allow privilege escalation.	2021-07-16	not yet calculated	CVE-2021-3550 MISC
lexmark -- printer_software_installation_packages	The Lexmark Printer Software G2, G3 and G4 Installation Packages have a local escalation of privilege vulnerability due to a registry entry that has an unquoted service path.	2021-07-14	not yet calculated	CVE-2021-35469 MISC MISC
libvips -- libvips	Division-By-Zero vulnerability in Libvips 8.10.5 in the function vips_eye_point, eye.c#L83, and function vips_mask_point, mask.c#L85.	2021-07-15	not yet calculated	CVE-2021-27847 MISC
magicmotion -- flamingo_2	The MagicMotion Flamingo 2 application for Android stores data on an sdcard under com.vt.magicmotion/files/Pictures, whence it can be read by other applications.	2021-07-15	not yet calculated	CVE-2020-12731 MISC
magicmotion -- flamingo_2	MagicMotion Flamingo 2 has a lack of access control for reading from device descriptors.	2021-07-15	not yet calculated	CVE-2020-12729 MISC
magicmotion -- flamingo_2	MagicMotion Flamingo 2 lacks BLE encryption, enabling data sniffing and packet forgery.	2021-07-15	not yet calculated	CVE-2020-12730 MISC
mendix -- mendix	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.22), Mendix Applications using Mendix 8 (All versions < V8.18.7), Mendix Applications using Mendix 9 (All versions < V9.3.0). Write access checks of attributes of an object could be bypassed, if user has a write permissions to the first attribute of this object.	2021-07-13	not yet calculated	CVE-2021-33718 CONFIRM
micronaut -- micronaut	Micronaut is a JVM-based, full stack Java framework designed for building JVM applications. A path traversal vulnerability exists in versions prior to 2.5.9. With a basic configuration, it is possible to access any file from a filesystem, using "/../../" in the URL. This occurs because Micronaut does not restrict file access to configured paths. The vulnerability is patched in version 2.5.9. As a workaround, do not use `**` in mapping, use only `*`, which exposes only flat structure of a directory not allowing traversal. If using Linux, another workaround is to run micronaut in chroot.	2021-07-16	not yet calculated	CVE-2021-32769 CONFIRM MISC
microsoft -- defender	Microsoft Defender Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34464.	2021-07-14	not yet calculated	CVE-2021-34522 MISC
microsoft -- directwrite	DirectWrite Remote Code Execution Vulnerability	2021-07-14	not yet calculated	CVE-2021-34489 MISC
microsoft -- dynamics	Dynamics Business Central Remote Code Execution Vulnerability	2021-07-14	not yet calculated	CVE-2021-34474 MISC
microsoft -- excel	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34518.	2021-07-14	not yet calculated	CVE-2021-34501 MISC
microsoft -- excel	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34501.	2021-07-14	not yet calculated	CVE-2021-34518 MISC
microsoft -- exchange	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34523.	2021-07-14	not yet calculated	CVE-2021-34470 MISC
microsoft -- exchange	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-31206.	2021-07-14	not yet calculated	CVE-2021-34473 MISC
microsoft -- exhange	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34470.	2021-07-14	not yet calculated	CVE-2021-34523 MISC
microsoft -- office	Microsoft Office Security Feature Bypass Vulnerability	2021-07-14	not yet calculated	CVE-2021-34469 MISC
microsoft -- office	Microsoft Office Online Server Spoofing Vulnerability	2021-07-16	not yet calculated	CVE-2021-34451 MISC
microsoft -- sharepoint	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34467, CVE-2021-34468.	2021-07-14	not yet calculated	CVE-2021-34520 MISC
microsoft -- sharepoint	Microsoft SharePoint Server Information Disclosure Vulnerability	2021-07-14	not yet calculated	CVE-2021-34519 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- sharepoint	Microsoft SharePoint Server Spoofing Vulnerability	2021-07-14	not yet calculated	CVE-2021-34517 MISC
microsoft -- sharepoint	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34467, CVE-2021-34520.	2021-07-14	not yet calculated	CVE-2021-34468 MISC
microsoft -- sharepoint	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34468, CVE-2021-34520.	2021-07-16	not yet calculated	CVE-2021-34467 MISC
microsoft -- thinkpad	A potential vulnerability in the system shutdown SMI callback function in some ThinkPad models may allow an attacker with local access and elevated privileges to execute arbitrary code.	2021-07-16	not yet calculated	CVE-2021-3452 MISC
microsoft -- visual_studio	Visual Studio Code .NET Runtime Elevation of Privilege Vulnerability	2021-07-14	not yet calculated	CVE-2021-34477 MISC
microsoft -- visual_studio	Microsoft Visual Studio Spoofing Vulnerability	2021-07-14	not yet calculated	CVE-2021-34479 MISC
microsoft -- visual_studio	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34528.	2021-07-14	not yet calculated	CVE-2021-34529 MISC
microsoft -- visual_studio	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34529.	2021-07-14	not yet calculated	CVE-2021-34528 MISC
microsoft -- win32k	Win32k Information Disclosure Vulnerability	2021-07-14	not yet calculated	CVE-2021-34491 MISC
microsoft -- win32k	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34516.	2021-07-16	not yet calculated	CVE-2021-34449 MISC
microsoft -- win32k	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34449.	2021-07-14	not yet calculated	CVE-2021-34516 MISC
microsoft -- windows	Windows Remote Access Connection Manager Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-33763, CVE-2021-34457.	2021-07-16	not yet calculated	CVE-2021-34454 MISC
microsoft -- windows	Windows Remote Access Connection Manager Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-33763, CVE-2021-34454.	2021-07-16	not yet calculated	CVE-2021-34457 MISC
microsoft -- windows	Windows MSHTML Platform Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34497.	2021-07-16	not yet calculated	CVE-2021-34447 MISC
microsoft -- windows	Scripting Engine Memory Corruption Vulnerability	2021-07-16	not yet calculated	CVE-2021-34448 MISC
microsoft -- windows	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33745, CVE-2021-34442, CVE-2021-34499.	2021-07-16	not yet calculated	CVE-2021-34444 MISC
microsoft -- windows	Windows GDI Information Disclosure Vulnerability	2021-07-14	not yet calculated	CVE-2021-34496 MISC
microsoft -- windows	Windows Certificate Spoofing Vulnerability	2021-07-14	not yet calculated	CVE-2021-34492 MISC
microsoft -- windows	Windows Kernel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34508.	2021-07-16	not yet calculated	CVE-2021-34458 MISC
microsoft -- windows	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability	2021-07-16	not yet calculated	CVE-2021-34461 MISC
microsoft -- windows	Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34503.	2021-07-16	not yet calculated	CVE-2021-34441 MISC
microsoft -- windows	Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34441, CVE-2021-34503.	2021-07-16	not yet calculated	CVE-2021-34439 MISC
microsoft -- windows	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33751, CVE-2021-34510, CVE-2021-34512, CVE-2021-34513.	2021-07-16	not yet calculated	CVE-2021-34460 MISC
microsoft -- windows	GDI+ Information Disclosure Vulnerability	2021-07-16	not yet calculated	CVE-2021-34440 MISC
microsoft -- windows	Windows HTML Platforms Security Feature Bypass Vulnerability	2021-07-16	not yet calculated	CVE-2021-34446 MISC
microsoft -- windows	Windows File History Service Elevation of Privilege Vulnerability	2021-07-16	not yet calculated	CVE-2021-34455 MISC
microsoft -- windows	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-33773, CVE-2021-34445.	2021-07-16	not yet calculated	CVE-2021-34456 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33745, CVE-2021-34444, CVE-2021-34499.	2021-07-16	not yet calculated	CVE-2021-34442 MISC
microsoft -- windows	Microsoft Defender Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34522.	2021-07-16	not yet calculated	CVE-2021-34464 MISC
microsoft -- windows	Windows Print Spooler Elevation of Privilege Vulnerability	2021-07-16	not yet calculated	CVE-2021-34481 MISC
microsoft -- windows	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	2021-07-16	not yet calculated	CVE-2021-34462 MISC
microsoft -- windows	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-31183, CVE-2021-33772.	2021-07-14	not yet calculated	CVE-2021-34490 MISC
microsoft -- windows	Windows Console Driver Elevation of Privilege Vulnerability	2021-07-14	not yet calculated	CVE-2021-34488 MISC
microsoft -- windows	Windows Partition Management Driver Elevation of Privilege Vulnerability	2021-07-14	not yet calculated	CVE-2021-34493 MISC
microsoft -- windows	Bowser.sys Denial of Service Vulnerability	2021-07-14	not yet calculated	CVE-2021-34476 MISC
microsoft -- windows	Windows AppContainer Elevation Of Privilege Vulnerability	2021-07-16	not yet calculated	CVE-2021-34459 MISC
microsoft -- windows	Windows Hello Security Feature Bypass Vulnerability	2021-07-16	not yet calculated	CVE-2021-34466 MISC
microsoft -- windows	Windows Font Driver Host Remote Code Execution Vulnerability	2021-07-16	not yet calculated	CVE-2021-34438 MISC
microsoft -- windows	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-33773, CVE-2021-34456.	2021-07-16	not yet calculated	CVE-2021-34445 MISC
microsoft -- windows	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33754, CVE-2021-33780, CVE-2021-34525.	2021-07-14	not yet calculated	CVE-2021-34494 MISC
microsoft -- windows	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33751, CVE-2021-34460, CVE-2021-34510, CVE-2021-34513.	2021-07-14	not yet calculated	CVE-2021-34512 MISC
microsoft -- windows	Windows GDI Elevation of Privilege Vulnerability	2021-07-14	not yet calculated	CVE-2021-34498 MISC
microsoft -- windows	Windows Hyper-V Remote Code Execution Vulnerability	2021-07-16	not yet calculated	CVE-2021-34450 MISC
microsoft -- windows	Windows MSHTML Platform Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34447.	2021-07-14	not yet calculated	CVE-2021-34497 MISC
microsoft -- windows	Windows Kernel Memory Information Disclosure Vulnerability	2021-07-14	not yet calculated	CVE-2021-34500 MISC
microsoft -- windows	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33751, CVE-2021-34460, CVE-2021-34510, CVE-2021-34512.	2021-07-14	not yet calculated	CVE-2021-34513 MISC
microsoft -- windows	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33754, CVE-2021-33780, CVE-2021-34494.	2021-07-14	not yet calculated	CVE-2021-34525 MISC
microsoft -- windows	Raw Image Extension Remote Code Execution Vulnerability	2021-07-14	not yet calculated	CVE-2021-34521 MISC
microsoft -- windows	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33745, CVE-2021-34442, CVE-2021-34444.	2021-07-14	not yet calculated	CVE-2021-34499 MISC
microsoft -- windows	Windows Address Book Remote Code Execution Vulnerability	2021-07-14	not yet calculated	CVE-2021-34504 MISC
microsoft -- windows	Windows Remote Assistance Information Disclosure Vulnerability	2021-07-14	not yet calculated	CVE-2021-34507 MISC
microsoft -- windows	Windows Kernel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34458.	2021-07-14	not yet calculated	CVE-2021-34508 MISC
microsoft -- windows	Storage Spaces Controller Information Disclosure Vulnerability	2021-07-14	not yet calculated	CVE-2021-34509 MISC
microsoft -- windows	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33751, CVE-2021-34460, CVE-2021-34512, CVE-2021-34513.	2021-07-14	not yet calculated	CVE-2021-34510 MISC
microsoft -- windows	Windows Installer Elevation of Privilege Vulnerability	2021-07-14	not yet calculated	CVE-2021-34511 MISC
microsoft -- windows	Windows Kernel Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31979, CVE-2021-33771.	2021-07-14	not yet calculated	CVE-2021-34514 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows	Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34441.	2021-07-14	not yet calculated	CVE-2021-34503 MISC
microsoft -- windows_server	Windows LSA Denial of Service Vulnerability	2021-07-14	not yet calculated	CVE-2021-33788 MISC
microsoft -- windows_server	Windows LSA Security Feature Bypass Vulnerability	2021-07-14	not yet calculated	CVE-2021-33786 MISC
microsoft -- word	Microsoft Word Remote Code Execution Vulnerability	2021-07-16	not yet calculated	CVE-2021-34452 MISC
miktorik -- routeros	Mikrotik RouterOs through stable version 6.48.3 suffers from a memory corruption vulnerability in the /nova/bin/detnet process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-07-14	not yet calculated	CVE-2020-20231 MISC MISC
mitsubishi -- electric_air_conditioning_system	Incorrect Implementation of Authentication Algorithm in Mitsubishi Electric Air Conditioning System/Centralized Controllers (G-50A Ver.2.50 to Ver. 3.35, GB-50A Ver.2.50 to Ver. 3.35, AG-150A-A Ver.3.20 and prior, AG-150A-J Ver.3.20 and prior, GB-50ADA-A Ver.3.20 and prior, GB-50ADA-J Ver.3.20 and prior, EB-50GU-A Ver 7.09 and prior, EB-50GU-J Ver 7.09 and prior, AE-200A Ver 7.93 and prior, AE-200E Ver 7.93 and prior, AE-50A Ver 7.93 and prior, AE-50E Ver 7.93 and prior, EW-50A Ver 7.93 and prior, EW-50E Ver 7.93 and prior, TE-200A Ver 7.93 and prior, TE-50A Ver 7.93 and prior, TW-50A Ver 7.93 and prior, CMS-RMD-J Ver.1.30 and prior) and Air Conditioning System/Expansion Controllers (PAC-YG50ECA Ver.2.20 and prior) allows a remote authenticated attacker to impersonate administrators to disclose configuration information of the air conditioning system and tamper information (e.g. operation information and configuration of air conditioning system) by exploiting this vulnerability.	2021-07-13	not yet calculated	CVE-2021-20593 MISC MISC
mitsubishi -- electric_air_conditioning_system	Improper Restriction of XML External Entity Reference vulnerability in Mitsubishi Electric Air Conditioning System/Centralized Controllers (G-50A Ver.3.35 and prior, GB-50A Ver.3.35 and prior, GB-24A Ver.9.11 and prior, AG-150A-A Ver.3.20 and prior, AG-150A-J Ver.3.20 and prior, GB-50ADA-A Ver.3.20 and prior, GB-50ADA-J Ver.3.20 and prior, EB-50GU-A Ver 7.09 and prior, EB-50GU-J Ver 7.09 and prior, AE-200A Ver 7.93 and prior, AE-200E Ver 7.93 and prior, AE-50A Ver 7.93 and prior, AE-50E Ver 7.93 and prior, EW-50A Ver 7.93 and prior, EW-50E Ver 7.93 and prior, TE-200A Ver 7.93 and prior, TE-50A Ver 7.93 and prior, TW-50A Ver 7.93 and prior, CMS-RMD-J Ver.1.30 and prior), Air Conditioning System/Expansion Controllers (PAC-YG50ECA Ver.2.20 and prior) and Air Conditioning System/BM adapter(BAC-HD150 Ver.2.21 and prior) allows a remote unauthenticated attacker to disclose some of data in the air conditioning system or cause a DoS condition by sending specially crafted packets.	2021-07-13	not yet calculated	CVE-2021-20595 MISC MISC
nightscout -- web_monitor	Nightscout Web Monitor (aka cgm-remote-monitor) 14.2.2 allows XSS via a crafted X-Forwarded-For header.	2021-07-16	not yet calculated	CVE-2021-36755 MISC
ok-file-formats -- ok-file-formats	A heap-based buffer overflow vulnerability in the function ok_jpg_decode_block_progressive() at ok_jpg.c:1054 of ok-file-formats through 2020-06-26 allows attackers to cause a Denial of Service (DOS) via a crafted jpeg file.	2021-07-15	not yet calculated	CVE-2020-23707 MISC
ok-file-formats -- ok-file-formats	A heap-based buffer overflow vulnerability in the function ok_jpg_decode_block_subsequent_scan() ok_jpg.c:1102 of ok-file-formats through 2020-06-26 allows attackers to cause a Denial of Service (DOS) via a crafted jpeg file.	2021-07-15	not yet calculated	CVE-2020-23706 MISC
palo_alto_networks -- cortex_xdr	A local privilege escalation (PE) vulnerability exists in the Palo Alto Networks Cortex XDR agent on Windows platforms that enables an authenticated local Windows user to execute programs with SYSTEM privileges. Exploiting this vulnerability requires the user to have file creation privilege in the Windows root directory (such as C:\). This issue impacts: All versions of Cortex XDR agent 6.1 without content update 181 or a later version; All versions of Cortex XDR agent 7.2 without content update 181 or a later version; All versions of Cortex XDR agent 7.3 without content update 181 or a later version. Cortex XDR agent 5.0 versions are not impacted by this issue. Content updates are required to resolve this issue and are automatically applied for the agent.	2021-07-15	not yet calculated	CVE-2021-3042 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
polipo -- polipo	** UNSUPPORTED WHEN ASSIGNED ** Polipo through 1.1.1 allows denial of service via a reachable assertion during parsing of a malformed Range header. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-07-15	not yet calculated	CVE-2020-36420 MISC MISC MISC
prisma -- cloud_compute	A reflected cross-site scripting (XSS) vulnerability exists in the Prisma Cloud Compute web console that enables a remote attacker to execute arbitrary JavaScript code in the browser-based web console while an authenticated administrator is using that web interface. Prisma Cloud Compute SaaS versions were automatically upgraded to the fixed release. No additional action is required for these instances. This issue impacts: Prisma Cloud Compute 20.12 versions earlier than Prisma Cloud Compute 20.12.552; Prisma Cloud Compute 21.04 versions earlier than Prisma Cloud Compute 21.04.439.	2021-07-15	not yet calculated	CVE-2021-3043 MISC
radarorg -- radare2-extras	A heap buffer overflow vulnerability in the r_asm_swf_disass function of Radare2-extras before commit e74a93c allows attackers to execute arbitrary code or carry out denial of service (DOS) attacks.	2021-07-14	not yet calculated	CVE-2020-24133 MISC MISC MISC
rancher -- rancher	A Improper Access Control vulnerability in Rancher, allows users in the cluster to make request to cloud providers by creating requests with the cloud-credential ID. Rancher in this case would attach the requested credentials without further checks This issue affects: Rancher versions prior to 2.5.9; Rancher versions prior to 2.4.16.	2021-07-15	not yet calculated	CVE-2021-25320 CONFIRM
rancher -- rancher	A Incorrect Permission Assignment for Critical Resource vulnerability in Rancher allows users in the cluster to modify resources they should not have access to. This issue affects: Rancher versions prior to 2.5.9 ; Rancher versions prior to 2.4.16.	2021-07-15	not yet calculated	CVE-2021-25318 CONFIRM
rancher -- rancher	A Reliance on Untrusted Inputs in a Security Decision vulnerability in Rancher allows users in the cluster to act as others users in the cluster by forging the "Impersonate-User" or "Impersonate-Group" headers. This issue affects: Rancher versions prior to 2.5.9. Rancher versions prior to 2.4.16.	2021-07-15	not yet calculated	CVE-2021-31999 CONFIRM
raonwiz -- editor	An issue in RAONWIZ K Editor v2018.0.0.10 allows attackers to perform a DLL hijacking attack when the service or system is restarted.	2021-07-14	not yet calculated	CVE-2020-29157 MISC MISC
ruby -- ruby	An issue was discovered in Ruby through 2.6.7, 2.7.x through 2.7.3, and 3.x through 3.0.1. A malicious FTP server can use the PASV response to trick Net::FTP into connecting back to a given IP address and port. This potentially makes curl extract information about services that are otherwise private and not disclosed (e.g., the attacker can conduct port scans and service banner extractions).	2021-07-13	not yet calculated	CVE-2021-31810 MISC MISC
rust -- sgx	In Rust SGX 1.1.3, a side-channel vulnerability in base64 PEM file decoding allows system-level (administrator) attackers to obtain information about secret RSA keys via a controlled-channel and side-channel attack on software running in isolated environments that can be single stepped, especially Intel SGX.	2021-07-14	not yet calculated	CVE-2021-24117 MISC MISC MISC
rwg1.m12 -- rwg1.m12	A vulnerability has been identified in RWG1.M12 (All versions < V1.16.16), RWG1.M12D (All versions < V1.16.16), RWG1.M8 (All versions < V1.16.16). Sending specially crafted ARP packets to an affected device could cause a partial denial-of-service, preventing the device to operate normally. A restart is needed to restore normal operations.	2021-07-13	not yet calculated	CVE-2021-25671 CONFIRM
sap -- netweaver	SAP NetWeaver AS ABAP and ABAP Platform, versions - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.77, 7.81, 7.84, allows an attacker to send overlong content in the RFC request type thereby crashing the corresponding work process because of memory corruption vulnerability. The work process will attempt to restart itself after the crash and hence the impact on the availability is low.	2021-07-14	not yet calculated	CVE-2021-33684 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- web_dispatcher_and_internet_communication_manager	SAP Web Dispatcher and Internet Communication Manager (ICM), versions - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.73, WEBDISP 7.53, 7.73, 7.77, 7.81, 7.82, 7.83, KERNEL 7.21, 7.22, 7.49, 7.53, 7.73, 7.77, 7.81, 7.82, 7.83, process invalid HTTP header. The incorrect handling of the invalid Transfer-Encoding header in a particular manner leads to a possibility of HTTP Request Smuggling attack. An attacker could exploit this vulnerability to bypass web application firewall protection, divert sensitive data such as customer requests, session credentials, etc.	2021-07-14	not yet calculated	CVE-2021-33683 MISC MISC
sharkdp -- bat	sharkdp BAT before 0.18.2 executes less.exe from the current working directory.	2021-07-15	not yet calculated	CVE-2021-36753 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- multiple_products	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All versions), RUGGEDCOM RM1224 (All Versions < 6.4), SCALANCE M-800 (All Versions < 6.4), SCALANCE S615 (All Versions < 6.4), SCALANCE W1700 IEEE 802.11ac (All versions), SCALANCE W700 IEEE 802.11n (All versions), SCALANCE X200-4 P IRT (All Versions < V5.5.0), SCALANCE X201-3P IRT (All Versions < V5.5.0), SCALANCE X201-3P IRT PRO (All Versions < V5.5.0), SCALANCE X202-2 IRT (All Versions < V5.5.0), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All Versions < V5.5.0), SCALANCE X202-2P IRT PRO (All Versions < V5.5.0), SCALANCE X204 IRT (All Versions < V5.5.0), SCALANCE X204 IRT PRO (All Versions < V5.5.0), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (incl. SIPLUS NET variant) (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE X302-7EEC (All versions), SCALANCE X304-2FE (All versions), SCALANCE X306-1LDFE (All versions), SCALANCE X307-2EEC (All versions), SCALANCE X307-3 (All versions), SCALANCE X307-3LD (All versions), SCALANCE X308-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X308-2LD (All versions), SCALANCE X308-2LH (All versions), SCALANCE X308-2LH+ (All versions), SCALANCE X308-2M (All versions), SCALANCE X308-2M POE (All versions), SCALANCE X308-2M TS (All versions), SCALANCE X310 (All versions), SCALANCE X310FE (All versions), SCALANCE X320-1FE (All versions), SCALANCE X320-3LDFE (All versions), SCALANCE XB-200 (All versions), SCALANCE XC-200 (All versions), SCALANCE XF-200BA (All versions), SCALANCE XF201-3P IRT (All Versions < V5.5.0), SCALANCE XF202-2P IRT (All Versions < V5.5.0), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All Versions < V5.5.0), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All Versions < V5.5.0), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions), SCALANCE XM400 (All versions < V6.3.1), SCALANCE XP-200 (All versions), SCALANCE XR-300WG (All versions), SCALANCE XR324-12M (All versions), SCALANCE XR324-12M TS (All versions), SCALANCE XR324-4M EEC (All versions), SCALANCE XR324-4M POE (All versions), SCALANCE XR324-4M POE TS (All versions), SCALANCE XR500 (All versions < V6.3.1), SIMATIC CFU PA (All versions), SIMATIC IE/PB-LINK V3 (All versions), SIMATIC MV500 family (All versions < V3.0), SIMATIC NET CM 1542-1 (All versions), SIMATIC NET CP1616/CP1604 (All Versions >= V2.7), SIMATIC NET CP1626 (All versions), SIMATIC NET DK-16xx PN IO (All Versions >= V2.7), SIMATIC PROFINET Driver (All versions), SIMATIC Power Line Booster PLB, Base Module (MLFB: 6ES7972-5AA10-0AB0) (All versions), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All Versions < V4.5), SIMOCODE proV Ethernet/IP (All versions < V1.1.3), SIMOCODE proV PROFINET (All versions < V2.1.3), SOFTNET-IE PNIO (All versions). Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large amount of DCP reset packets are sent to the device.	2021-07-13	not yet calculated	CVE-2020-28400 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- sinumerik	A vulnerability has been identified in SINUMERIK Analyse MyCondition (All versions), SINUMERIK Analyze MyPerformance (All versions), SINUMERIK Analyze MyPerformance /OEE-Monitor (All versions), SINUMERIK Analyze MyPerformance /OEE-Tuning (All versions), SINUMERIK Integrate Client 02 (All versions >= V02.00.12 < 02.00.18), SINUMERIK Integrate Client 03 (All versions >= V03.00.12 < 03.00.18), SINUMERIK Integrate Client 04 (V04.00.02 and all versions >= V04.00.15 < 04.00.18), SINUMERIK Integrate for Production 4.1 (All versions < V4.1 SP10 HF3), SINUMERIK Integrate for Production 5.1 (V5.1), SINUMERIK Manage MyMachines (All versions), SINUMERIK Manage MyMachines /Remote (All versions), SINUMERIK Manage MyMachines /Spindel Monitor (All versions), SINUMERIK Manage MyPrograms (All versions), SINUMERIK Manage MyResources /Programs (All versions), SINUMERIK Manage MyResources /Tools (All versions), SINUMERIK Manage MyTools (All versions), SINUMERIK Operate V4.8 (All versions < V4.8 SP8), SINUMERIK Operate V4.93 (All versions < V4.93 HF7), SINUMERIK Operate V4.94 (All versions < V4.94 HF5), SINUMERIK Optimize MyProgramming /NX-Cam Editor (All versions). Due to an error in a third-party dependency the ssl flags used for setting up a TLS connection to a server are overwitten with wrong settings. This results in a missing validation of the server certificate and thus in a possible TLS MITM szenario.	2021-07-13	not yet calculated	CVE-2021-31892 CONFIRM
siemens -- simatic_pcs	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.X (All versions), SIMATIC PDM (All versions), SIMATIC STEP 7 V5.X (All versions < V5.7), SINAMICS STARTER (containing STEP 7 OEM version) (All versions). A directory containing metafiles relevant to devices' configurations has write permissions. An attacker could leverage this vulnerability by changing the content of certain metafiles and subsequently manipulate parameters or behavior of devices that would be later configured by the affected software.	2021-07-13	not yet calculated	CVE-2021-31894 CONFIRM
siemens -- simatic_pcs	A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3), SIMATIC PDM (All versions < V9.2), SIMATIC STEP 7 V5.X (All versions < V5.6 SP2 HF3), SINAMICS STARTER (containing STEP 7 OEM version) (All versions < V5.4 HF2). The affected software contains a buffer overflow vulnerability while handling certain files that could allow a local attacker to trigger a denial-of-service condition or potentially lead to remote code execution.	2021-07-13	not yet calculated	CVE-2021-31893 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- multiple_ruggedcomros_products	A vulnerability has been identified in RUGGEDCOM ROS M2100 (All versions < V4.3.7), RUGGEDCOM ROS M2200 (All versions < V4.3.7), RUGGEDCOM ROS M969 (All versions < V4.3.7), RUGGEDCOM ROS RMC (All versions < V4.3.7), RUGGEDCOM ROS RMC20 (All versions < V4.3.7), RUGGEDCOM ROS RMC30 (All versions < V4.3.7), RUGGEDCOM ROS RMC40 (All versions < V4.3.7), RUGGEDCOM ROS RMC41 (All versions < V4.3.7), RUGGEDCOM ROS RMC8388 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RMC8388 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RP110 (All versions < V4.3.7), RUGGEDCOM ROS RS400 (All versions < V4.3.7), RUGGEDCOM ROS RS401 (All versions < V4.3.7), RUGGEDCOM ROS RS416 (All versions < V4.3.7), RUGGEDCOM ROS RS416v2 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RS416v2 V5.X (All versions < 5.5.4), RUGGEDCOM ROS RS8000 (All versions < V4.3.7), RUGGEDCOM ROS RS8000A (All versions < V4.3.7), RUGGEDCOM ROS RS8000H (All versions < V4.3.7), RUGGEDCOM ROS RS8000T (All versions < V4.3.7), RUGGEDCOM ROS RS900 (32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RS900 (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RS900G (All versions < V4.3.7), RUGGEDCOM ROS RS900G (32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RS900G (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RS900GP (All versions < V4.3.7), RUGGEDCOM ROS RS900L (All versions < V4.3.7), RUGGEDCOM ROS RS900W (All versions < V4.3.7), RUGGEDCOM ROS RS910 (All versions < V4.3.7), RUGGEDCOM ROS RS910L (All versions < V4.3.7), RUGGEDCOM ROS RS910W (All versions < V4.3.7), RUGGEDCOM ROS RS920L (All versions < V4.3.7), RUGGEDCOM ROS RS920W (All versions < V4.3.7), RUGGEDCOM ROS RS930L (All versions < V4.3.7), RUGGEDCOM ROS RS930W (All versions < V4.3.7), RUGGEDCOM ROS RS940G (All versions < V4.3.7), RUGGEDCOM ROS RS969 (All versions < V4.3.7), RUGGEDCOM ROS RSG2100 (32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2100 (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2100 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2100P (All versions < V4.3.7), RUGGEDCOM ROS RSG2100P (32M) V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2100P (32M) V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2200 (All versions < V4.3.7), RUGGEDCOM ROS RSG2288 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2288 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2300 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2300 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2300P V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2300P V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG2488 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG2488 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG900 V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG900 V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG900C (All versions < V5.5.4), RUGGEDCOM ROS RSG900G V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG900G V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSG900R (All versions < V5.5.4), RUGGEDCOM ROS RSG920P V4.X (All versions < V4.3.7), RUGGEDCOM ROS RSG920P V5.X (All versions < V5.5.4), RUGGEDCOM ROS RSL910 (All versions < V5.5.4), RUGGEDCOM ROS RST2228 (All versions < V5.5.4), RUGGEDCOM ROS RST916C (All versions < V5.5.4), RUGGEDCOM ROS RST916P (All versions < V5.5.4), RUGGEDCOM ROS i800 (All versions < V4.3.7), RUGGEDCOM ROS i801 (All versions < V4.3.7), RUGGEDCOM ROS i802 (All versions < V4.3.7), RUGGEDCOM ROS i803 (All versions < V4.3.7). The DHCP client in affected devices fails to properly sanitize incoming DHCP packets. This could allow an unauthenticated remote attacker to cause memory to be overwritten, potentially allowing remote code execution.	2021-07-13	not yet calculated	CVE-2021-31895 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solarwinds -- serv-u	Microsoft discovered a remote code execution (RCE) vulnerability in the SolarWinds Serv-U product utilizing a Remote Memory Escape Vulnerability. If exploited, a threat actor may be able to gain privileged access to the machine hosting Serv-U Only. SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP for Windows before 15.2.3 HF2 are affected by this vulnerability.	2021-07-14	not yet calculated	CVE-2021-35211 MISC MISC
teamcenter -- active_workspace	A vulnerability has been identified in Teamcenter Active Workspace V4 (All versions < V4.3.9), Teamcenter Active Workspace V5.0 (All versions < V5.0.7), Teamcenter Active Workspace V5.1 (All versions < V5.1.4). By sending malformed requests, a remote attacker could leak an application token due to an error not properly handled by the system.	2021-07-13	not yet calculated	CVE-2021-33709 CONFIRM
teamcenter -- active_workspace	A vulnerability has been identified in Teamcenter Active Workspace V4 (All versions < V4.3.9), Teamcenter Active Workspace V5.0 (All versions < V5.0.7), Teamcenter Active Workspace V5.1 (All versions < V5.1.4). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected devices that could allow an attacker to execute malicious JavaScript code by tricking users into accessing a malicious link.	2021-07-13	not yet calculated	CVE-2021-33710 CONFIRM
teamcenter -- active_workspace	A vulnerability has been identified in Teamcenter Active Workspace V4 (All versions < V4.3.9), Teamcenter Active Workspace V5.0 (All versions < V5.0.7), Teamcenter Active Workspace V5.1 (All versions < V5.1.4). The affected application allows verbose error messages which allow leaking of sensitive information, such as full paths.	2021-07-13	not yet calculated	CVE-2021-33711 CONFIRM
telegram -- telegram	A reordering issue exists in Telegram before 7.8.1 for Android, Telegram before 7.8.3 for iOS, and Telegram Desktop before 2.8.8. An attacker can cause the server to receive messages in a different order than they were sent a client.	2021-07-17	not yet calculated	CVE-2021-36769 MISC
thinkcmf -- thinkcmf	Cross Site Request Forgerly (CSRF) vulnerability in ThinkCMF v5.1.0, which can add an admin account.	2021-07-14	not yet calculated	CVE-2020-18151 MISC
trusted_firmware_mbed -- tls	In Trusted Firmware Mbed TLS 2.24.0, a side-channel vulnerability in base64 PEM file decoding allows system-level (administrator) attackers to obtain information about secret RSA keys via a controlled-channel and side-channel attack on software running in isolated environments that can be single stepped, especially Intel SGX.	2021-07-14	not yet calculated	CVE-2021-24119 MISC MISC
unisys -- stealth	Unisys Stealth 5.1 before 5.1.025.0 and 6.0 before 6.0.055.0 has an unquoted Windows search path for a scheduled task. An unintended executable might run.	2021-07-15	not yet calculated	CVE-2021-35056 MISC CONFIRM
uri.js -- uri.js	URI.js is vulnerable to URL Redirection to Untrusted Site	2021-07-16	not yet calculated	CVE-2021-3647 MISC CONFIRM
varnish -- cache	Varnish Cache, with HTTP/2 enabled, allows request smuggling and VCL authorization bypass via a large Content-Length header for a POST request. This affects Varnish Enterprise 6.0.x before 6.0.8r3, and Varnish Cache 5.x and 6.x before 6.5.2, 6.6.x before 6.6.1, and 6.0 LTS before 6.0.8.	2021-07-14	not yet calculated	CVE-2021-36740 MISC MISC MISC MISC
wolfssl -- wolfssl	In wolfSSL through 4.6.0, a side-channel vulnerability in base64 PEM file decoding allows system-level (administrator) attackers to obtain information about secret RSA keys via a controlled-channel and side-channel attack on software running in isolated environments that can be single stepped, especially Intel SGX.	2021-07-14	not yet calculated	CVE-2021-24116 MISC CONFIRM
wuwire -- wuwire	MuWire is a file publishing and networking tool that protects the identity of its users by using I2P technology. Users of MuWire desktop client prior to version 0.8.8 can be de-anonymized by an attacker who knows their full ID. An attacker could send a message with a subject line containing a URL with an HTML image tag and the MuWire client would try to fetch that image via clearnet, thus exposing the IP address of the user. The problem is fixed in MuWire 0.8.8. As a workaround, users can disable messaging functionality to prevent other users from sending them malicious messages.	2021-07-15	not yet calculated	CVE-2021-32750 CONFIRM
ysoft -- safeq	Incorrect privileges in the MU55 FlexiSpooler service in YSoft SafeQ 6 6.0.55 allows local user privilege escalation by overwriting the executable file via an alternative data stream.	2021-07-14	not yet calculated	CVE-2021-31859 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zoho_manageengine -- admanager_plus	Zoho ManageEngine ADManager Plus before 7110 allows remote code execution.	2021-07-17	not yet calculated	CVE-2021-33911 MISC
zoho_manageengine -- admanager_plus	Zoho ManageEngine ADManager Plus before 7110 allows reflected XSS.	2021-07-17	not yet calculated	CVE-2021-36771 MISC
zoho_manageengine -- admanager_plus	Zoho ManageEngine ADManager Plus before 7110 allows stored XSS.	2021-07-17	not yet calculated	CVE-2021-36772 MISC
zscaler -- client_connector	The Zscaler Client Connector for Windows prior to 2.1.2.74 had a stack based buffer overflow when connecting to misconfigured TLS servers. An adversary would potentially have been able to execute arbitrary code with system privileges.	2021-07-15	not yet calculated	CVE-2020-11633 MISC
zscaler -- client_connector	The Zscaler Client Connector prior to 2.1.2.150 did not quote the search path for services, which allows a local adversary to execute code with system privileges.	2021-07-15	not yet calculated	CVE-2020-11632 MISC
zscaler -- client_connector	The Zscaler Client Connector for Windows prior to 2.1.2.105 had a DLL hijacking vulnerability caused due to the configuration of OpenSSL. A local adversary may be able to execute arbitrary code in the SYSTEM context.	2021-07-15	not yet calculated	CVE-2020-11634 MISC

Back to top